2/2016

Datenschutz Nachrichten

39. Jahrgang
ISSN 0137-7767
12,00 Euro



■ Die Europäische Datenschutz-Grundverordnung – ein Überblick ■ Entscheidung des EuGH zum sog. Recht auf Vergessenwerden ■ Rote Linien eingehalten? Zur Verabschiedung der Datenschutz-Grundverordnung ■ Nachrichten ■ Rechtsprechung ■ Buchbesprechungen ■

Deutsche Vereinigung für Datenschutz e.V.
www.datenschutzverein.de

Inhalt

Termine



Sonntag, 18. September 2016
DVD-Vorstandssitzung
Kiel. Anmeldung in der Geschäftsstelle
dvd@datenschutzverein.de

Montag, 19. September 2016
ULD-Sommerakademie
Kiel
https://www.datenschutzzentrum.de/sommerakademie/

21. und 22. Oktober 2016
Geheimdienste vor Gericht:
Humboldt-Universität und Maxim Gorki Theater Berlin
http://www.ausgeschnueffelt.de

Samstag, 22. Oktober 2016
DVD-Vorstandssitzung
Bonn. Anmeldung in der Geschäftsstelle
dvd@datenschutzverein.de

Sonntag, 23. Oktober 2016
DVD-Mitgliederversammlung
Bonn.
dvd@datenschutzverein.de

Foto: Uwe Schlick / pixelio.de

DANA
Datenschutz Nachrichten
ISSN 0137-7767
39. Jahrgang, Heft 2

Herausgeber
Deutsche Vereinigung für Datenschutz e.V. (DVD)
DVD-Geschäftstelle:
Reuterstraße 157, 53113 Bonn
Tel. 0228-222498
IBAN: DE94 3705 0198 0019 0021 87
Sparkasse KölnBonn
E-Mail: dvd@datenschutzverein.de
www.datenschutzverein.de

Redaktion (ViSdP)
Frank Spaeing
c/o Deutsche Vereinigung für Datenschutz e.V. (DVD)
Reuterstraße. 157, 53113 Bonn
dvd@datenschutzverein.de
Den Inhalt namentlich gekennzeichneter Artikel verantworten die jeweiligen Autoren.

Layout und Satz
Frans Jozef Valenta, 53119 Bonn
valenta@datenschutzverein.de

Druck
Onlineprinters GmbH
Rudolf-Diesel-Straße 10
91413 Neustadt a. d. Aisch
www.diedruckerei.de
Tel. +49 (0)91 61 / 6 20 98 00
Fax +49 (0) 91 61 / 66 29 20

Bezugspreis
Einzelheft 12 Euro. Jahresabonnement 42 Euro (incl. Porto) für vier Hefte im Kalenderjahr. Für DVD-Mitglieder ist der Bezug kostenlos. Das Jahresabonnement kann zum 31. Dezember eines Jahres mit einer Kündigungsfrist von sechs Wochen gekündigt werden. Die Kündigung ist schriftlich an die DVD-Geschäftsstelle in Bonn zu richten.

Leserbriefe
Leserbriefe sind erwünscht. Deren Publikation sowie eventuelle Kürzungen bleiben vorbehalten.

Abbildungen, Fotos
Frans Jozef Valenta

Editorial

Liebe Leserinnen und Leser,

am 25.05.2016 ist die EU-Datenschutzgrundverordnung (DSGVO) in Kraft getreten (siehe dazu auch den einleitenden Artikel von Thilo Weichert in diesem Heft). Grund genug für uns, Ihnen mehrere Aspekte der neuen DSGVO genauer darzustellen. Hierzu konnten wir Artikel von Sabine Leutheusser-Schnarrenberger zum Recht auf Vergessen, von Robert Selk zu den neuen Anforderungen an Einwilligungen nach der DSGVO und von Werner Hülsmann zu den Anforderungen der DSGVO an den betrieblichen Datenschutz gewinnen.

Wir haben mit dieser Ausgabe der DANA den beteiligten Organisationen, Verbänden und Einzelpersonen, die sich in der DANA 3/2015 zu den roten Linien, die im Rahmen der Trilog-Verhandlungen zwischen EU-Parlament und EU-Rat nicht überschritten werden durften, geäußert hatten, die Gelegenheit gegeben, ihre damaligen Forderungen und die nun fertige DSGVO gegenüberzustellen. Fast alle Beteiligten haben auch in dieser Ausgabe wieder mitgewirkt, in ihren Beiträgen ein Resümee gezogen und mitunter auch gleich den deutschen Gesetzgebern noch Empfehlungen für die Ausgestaltung des BDSG-Ablösegesetzes mitgegeben.

Sich diesem Themenblock anschließend haben wir in dieser Ausgabe einen weiteren Artikel von Werner Hülsmann, der die (in der DSGVO enthaltenen) Gestaltungsspielräume für die nationalen Gesetzgeber und die dazugehörigen Planungen des Bundesministeriums des Inneren darstellt.

Neben dem gemeinsamen Positionspapier von Digitalcourage und DVD zur konkreten Ausgestaltung der Spielräume rundet ein Artikel von Frans Jozef Valenta zum BigBrotherAward 2016 die DANA ab.

Natürlich fehlen auch in dieser Ausgabe nicht Datenschutznachrichten aus dem In- und Ausland, Technik-Nachrichten und Meldungen zu aktueller Rechtsprechung.

Eine anregende und informative Lektüre wünscht Ihnen
Frank Spaeing

Autorinnen und Autoren dieser Ausgabe:

Werner Hülsmann

Vorstandsmitglied in der DVD, Mitglied des Beirats des Forum InformatikerInnen für Frieden und gesellschaftliche Verantwortung (FIfF) e.V., selbständiger Datenschutzberater, externer Datenschutzbeauftragter und Datenschutzsachverständiger, Ismaning und Berlin, huelsmann@datenschutzverein.de

Sabine Leutheusser-Schnarrenberger

Bundesjustizministerin a. D., Mitglied des Google Advisory Council zum Recht auf Vergessen, info@leutheusser-schnarrenberger.de

Dr. Robert Selk

Rechtsanwalt, Fachanwalt für IT-Recht und Datenschutzbeauftragter,Leiter des Fachausschusses „Datenschutz“ der Deutschen Gesellschaft für Recht und Informatik, selk@kanzlei-ssh.de

Frans Jozef Valenta

Grafik-Designer, Vorstandsmitglied in der DVD, valenta@datenschutzverein.de

Dr. Thilo Weichert

Ehemaliger Leiter des Unabhängigen Landeszentrums für Datenschutz Schleswig Holstein, Kiel, Vorstandsmitgied in der DVD, weichert@datenschutzexpertise.de

Thilo Weichert

Die Europäische Datenschutz-Grundverordnung – ein Überblick

1 Kurzgeschichte der Verordnung

Am 08.04.2016 beschlossen der Rat der Europäischen Union (EU) und am 14.04.2016 das Parlament der EU einen neuen Rechtsrahmen zum Schutz personenbezogener Daten in der Europäischen Union, auf die sich diese am 15.12.2015 mit der Kommission der EU im sog. Trilog geeinigt hatten. Dieser Rechtsrahmen hat zwei Bestandteile, eine Richtlinie für den Datenschutz in den Bereichen Justiz und Polizei sowie eine Europäische Datenschutz-Grundverordnung (EU-DSGVO). Das Kernstück des neuen Rechtsrahmens ist die EU-DSGVO, mit der die Europäische Datenschutzrichtlinie (EG-DSRl) aus dem Jahr 1995 abgelöst wird.

Der Diskussion über die EU-DSGVO lag ursprünglich ein Vorschlag der EU-Kommission vom 25.01.2012 zugrunde. Das EU-Parlament beschloss dann mit großer Mehrheit am 12.03.2014 eine Vielzahl von Änderungsvorschlägen. Mit Datum vom 15.06.2015 hatte sich der EU-Rat auf seine Haltung zur EU-DSGVO verständigt. Für die Erarbeitung und Aushandlung der EU-DSGVO war das informelle Trilog-Verfahren gewählt worden, mit dem die Einberufung eines komplexen und möglicherweise zeitlich nicht überschaubaren Vermittlungsverfahrens vermieden wurde.

Bevor die Kommission ihren Vorschlag vorgelegt hatte, waren in Bezug auf den geplanten Rechtsrahmen zwei Konsultationen durchgeführt worden und zwar die vom 09.07.2009 bis 31.12.2009 „zum Rechtsrahmen für das Grundrecht auf Schutz personenbezogener Daten" sowie vom 04.11.2010 bis 15.01.2011 „zum Gesamtkonzept der Kommission für den Datenschutz in der Europäischen Union". Ihr „Gesamtkonzept" hatte die EU-Kommission am 04.11.2010 vorgestellt. Der EU-Rat hatte am 24.02.2011 Schlussfolgerungen angenommen, in denen er das Reformvorhaben der Kommission unterstützte. Mit einer Entschließung vom 06.07.2011 hatte das EU-Parlament einen Bericht angenommen, der das Kommissionskonzept für die Reform der Datenschutzregelungen guthieß.

2 Rechtlicher Rahmen

Die Vorschriften der nun verabschiedeten Grundverordnung zielen auf zweierlei ab: auf den Schutz des Grundrechts auf Datenschutz und auf die Garantie des freien Verkehrs personenbezogener Daten zwischen den Mitgliedstaaten.

In Art. 16 Abs. 1 des Vertrags über die Arbeitsweise der Europäischen Union (AEUV) ist der Grundsatz verankert, dass jede Person das Recht auf Schutz ihrer personenbezogenen Daten hat. Seit dem Vertrag von Lissabon verfügt die EU mit Art. 16 Abs. 2 AEUV über eine besondere Rechtsgrundlage für den Erlass von Datenschutzvorschriften.

Der europäische Rechtsrahmen zum Datenschutz in der EU hat zwei völkerrechtliche bzw. verfassungsrechtliche Grundlagen, nämlich Art. 8 der Europäischen Menschenrechtskonvention (EMRK) sowie die Art. 7 und 8 der Europäischen Grundrechtecharta (EuGRCh).

3 Zielsetzungen

Zur Erreichung der Rechtsetzungsziele – einem hohen Datenschutzstandard und dem freien Fluss personenbezogener Daten im Binnenmarkt – schälten sich im Laufe der Diskussionen über die EU-DSGVO folgende Zwischenziele hieraus:

- Es werden *einheitliche verbindliche Regelungen* angestrebt, die europaweit gelten und direkt anwendbar sind.
- Für die Anwendbarkeit der EU-DSGVO soll das *Marktortprinzip* gelten; d. h. die europäischen Verbraucher und Betroffenen sollen durch das für sie vor Ort geltende europäische Recht geschützt werden, unabhängig davon, wo die Datenverarbeitung erfolgt und wo der Sitz der verarbeitenden Stelle liegt.
- Über den sog. *One-Stop-Shop* soll für ein Unternehmen vorrangig die örtliche Datenschutzbehörde zuständig sein, so dass eine Kommunikation in einer konkreten Frage zum Datenschutz ausschließlich mit dieser erfolgt. Die Abstimmung der Position dieser Aufsichtsbehörde mit den anderen Aufsichtsbehörden, in deren Zuständigkeit ein Unternehmen auf dem Markt agiert, hat innerhalb des administrativen Bereichs zu erfolgen.
- Die *Transparenz für die Betroffenen* soll verbessert und den modernen technischen Gegebenheiten angepasst werden.
- Der *technische Datenschutz* soll durch neue Instrumente verbessert werden, bei denen die Prinzipien des Privacy by Design und Privacy by Default sowie der Datensparsamkeit schon bei der Technikgestaltung berücksichtigt werden.
- Über eine *Risikofolgenabschätzung* soll zwischen risikoreichen Anwendungen und sonstigen Verfahren differenziert werden. Bei geringerem Risiko soll für die Unternehmen der bürokratische Aufwand reduziert werden, während bei komplexen Verfahren ein adäquater Schutz angestrebt wird.
- Nicht nur der Datenaustausch innerhalb der EU bzw. des Binnenmarktes soll gefördert werden, sondern auch mit Staaten, in denen ein angemessener Datenschutz besteht. Fehlt dieser, so sind verbindliche und rechtssichere *Instrumente für den Drittland-Datentransfer* vorgesehen.

- Durch Verbesserung der Rechte der Betroffenen und deren Möglichkeit, durch *administrative und gerichtliche Verfahren* Rechtsschutz zu erlangen, sollen die bestehenden Vollzugsdefizite abgebaut werden.
- Über präventiv wie auch repressiv wirkende angemessen hohe *Sanktionen* soll die Bereitschaft zur Umsetzung des Datenschutzes und zur Compliance bei den verantwortlichen Stellen gefördert werden.

4 Struktur des EU-DSGVO

Die Grundverordnung ist in 11 Kapitel gegliedert, deren Struktur sich weitgehend an den bestehenden Datenschutzgesetzen und der EG-DSRl orientiert. Einen Schwerpunkt und Innovationen setzt die Verordnung weniger im materiell-rechtlichen Bereich als im administrativen, im technisch-organisatorischen sowie im prozeduralen Bereich. Die verbindlich geltende EU-DSGVO soll künftig an der Spitze einer hierarchischen Regelungsstruktur stehen, in der nationale Gesetze oder andere nachgeordnete Normen und Festlegungen spezielle Präzisierungen vornehmen können.

Die Zählweise der Artikel orientierte sich während der Diskussion in den EU-Gremien an den Vorgaben der EU-Kommission. Da jedoch ganze Artikel und Absätze gestrichen und andere hinzugefügt wurden, erfolgte vor der Beschlussfassung eine neue Durchnummerierung. Im folgenden Text werden die Artikel gemäß der endgültigen Beschlussfassung nummeriert.

Gliederung EU-DSGVO (Ziffern vor dem Schrägstrich Beschlussfassung/dahinter in der Entwurfsfassung)

Kap. 1 Allgemeine Bestimmungen (1-4)
Kap. 2 Grundsätze (5-11/5-10)
Kap. 3 Rechte der Betroffenen Person (12-23/11-21)
Kap. 4 Für Verarbeitung Verantwortlicher und Auftragsdatenverarbeiter (24-43/22-39a)
Kap. 5 Übermittlung personenbezogener Daten an Drittländer oder an internationale Organisationen (44-50/40-45)
Kap. 6 Unabhängigkeit der Aufsichtsbehörden (51-59/46-54)
Kap. 7 Zusammenarbeit und Kohärenz (60-76/54a-72)
Kap. 8 Rechtsbehelfe, Haftung und Sanktionen (77-84/73-79b)
Kap. 9 Besondere Datenverarbeitungssituationen (85-91/80-85)
Kap. 10 Delegierte Rechtsakte und Durchführungsrechtsakte (92, 93/86, 87)
Kap. 11 Schlussbestimmungen (94-99/88-91)

5 Anwendungsbereich

Die EU-DSGVO wird die zentrale Datenschutzregelung in der EU, ist aber nicht in allen Bereichen in der EU anwendbar. Dort, wo Unionsrecht keine Gültigkeit hat, gilt auch die EU-DSGVO nicht. Entsprechendes gilt für Tätigkeiten nach Titel V Kapitel 2 EUV, also die gemeinsame Außen- und Sicherheitspolitik. Für Tätigkeiten zum Zweck der polizeilichen und justiziellen Verhütung und Verfolgung von Straftaten gilt die zeitgleich konsentierte EU-Datenschutzrichtlinie für Justiz und Polizei. Weitere Ausnahmen sind die personenbezogene Verarbeitung von Daten in ungeordneten Akten sowie, wenn sich die Datenverarbeitung ausschließlich auf den persönlichen oder familiären Bereich bezieht (sog. Haushaltsausnahme). Soweit Organe der EU tätig werden, gilt weiterhin die Verordnung EG Nr. 45/2001. Unberührt bleibt weiterhin die Datenschutzrichtlinie für den Telekommunikationsbereich, welche die Verarbeitung von Bestands- und Verkehrsdaten von Netzdiensteanbietern regelt (Art. 2).

Es gilt das Marktortprinzip. Danach kommt es nicht darauf an, wo physisch die Datenverarbeitung erfolgt. Relevant ist vielmehr, dass die Verarbeitung einer verantwortlichen Stelle oder eines Auftragsdatenverarbeiters auf eine Person abzielt, die sich in der EU aufhält (Art. 3).

Die Begriffsbestimmungen bringen im Vergleich zur EG-DSRl keine wesentlichen inhaltlichen Änderungen, wohl aber Erweiterungen: Neu definiert werden z. B. Begriffe wie „Profiling", „Pseudonymisierung", „genetische Daten", „biometrische Daten", „Hauptniederlassung", „Vertreter", „Unternehmen", „Unternehmensgruppe" oder „verbindliche unternehmensinterne Datenschutzvorschriften", was bisher mit dem englischen Begriff „Binding Corporate Rules" (BCRs) bezeichnet worden ist (Art. 4).

6 Grundprinzipien

Im deutschen Datenschutzrecht war es bisher nicht üblich, Gesetzen *Grundprinzipien* voranzustellen, anders nun in Europa in Art. 5. Dies ist systematisch zu begrüßen. Bei der Auslegung der weiteren Regelungen sollte und kann immer hierauf zurückgegriffen werden. Außerdem wird dem mit dem Datenschutzrecht nicht vertrauten Menschen kurz und bündig klargestellt, welche generellen Erwägungen die EU-DSGVO prägen. Diese sind für erfahrene Anwender alle keine Unbekannten:

- Rechtmäßigkeit, Verarbeitung nach Treu und Glauben, Transparenz,
- Zweckbindung,
- Richtigkeit,
- Erforderlichkeit, die etwas sperrig „Speicherbegrenzung" genannt wird,
- Integrität und Vertraulichkeit,
- Verantwortlichkeit, die unter dem Begriff „Rechenschaftspflicht" geführt wird.

Hervorzuheben ist, dass als weiterer Grundsatz die *„Datenminimierung"* erwähnt wird. Wirtschaftsvertreter wie auch die deutsche Bundesregierung hatten noch kurz vor Abschluss des Trilogs dafür gekämpft, das Prinzip der Datensparsamkeit aus der EU-DSGVO zu verbannen, weil damit die Chancen der europäischen Wirtschaft bei der Entwicklung zukunftsweisender und lukrativer Big-Data-Konzepte beschnitten würden. Davon unbeeindruckt findet sich dieser Grundsatz nicht nur eingangs prominent, sondern an vielen weiteren Stellen, so insbesondere in Art. 25, wo als Instrumente der Datenminimierung die Pseudonymisierung und „Privacy by Default" genannt werden, im Rahmen von Zertifizierungen (Art. 25 Abs. 3), als Sicherheitsmaßnahme (Art. 32 Abs. 1 lit. a) sowie als Kriterium für Verhaltensregeln (Art. 40 Abs. 2 lit. d). In Art. 11 wird explizit klargestellt, dass aus einer pseudonymen oder sonstwie datensparsamen Verarbeitung keine Pflicht besteht, allein zum Zweck der Einhaltung der Verordnung zusätzliche Daten einzuholen.

Das schon bisher in der EG-DSRl geltende Verbot mit Erlaubnisvorbehalt ergibt sich aus Art. 6, der die *„Rechtmäßigkeit der Verarbeitung“* regelt. Übersichtlicher und systematischer als z. B. in den §§ 28 ff. BDSG werden die Legitimationsmöglichkeiten für die Verarbeitung aufgezählt:

- Einwilligung,
- Vertragserfüllung,
- Erfüllung einer rechtlichen Verpflichtung
- Schutz lebenswichtiger Interessen,
- Erfüllung einer Aufgabe im öffentlichen Interesse oder in Ausübung öffentlicher Gewalt,
- Wahrnehmung berechtigter Interessen, sofern die schutzwürdigen Interessen nicht überwiegen.

Der letztgenannte Punkt war umstritten. Während Datenschützer für eine Eingrenzung der *berechtigten Interessen* plädierten, setzten sich vor allem der Rat und die Wirtschaftslobby für eine Ausweitung ein. Letztendlich kam es insofern zu keiner Änderung des bisherigen Rechtszustands, der eine offene Abwägungsformel enthält (z. B. § 28 Abs. 1 S. 1 Nr. 2 BDSG).

Den Mitgliedstaaten wird in Art. 6 Abs. 3 und 4 insbesondere für die *Verarbeitung öffentlicher Stellen* und zur Erfüllung rechtlicher Pflichten ein sehr weitgehendes Konkretisierungsrecht zugesprochen. Dabei sind aber Regeln zu beachten: So muss eine klare Zweckbestimmung erkennbar sein. Eine Präzisierung kann hinsichtlich der Datenarten, der Verarbeitungsbedingungen, der Betroffenen, der verarbeitenden Stellen und der Speicherfristen erfolgen. Zu beachten ist, dass immer ein im öffentlichen Interesse liegendes Ziel in verhältnismäßiger Weise verfolgt wird.

Damit können die meisten in Deutschland geltenden *bereichsspezifischen Datenschutzregelungen* beibehalten werden. Die in der Verordnung genannten Anforderungen an solche bereichsspezifischen Regelungen entsprechen denen des deutschen Bundesverfassungsgerichts (BVerfG) an die Verfassungsmäßigkeit gesetzlicher Regelungen zur personenbezogenen Datenverarbeitung. Dies hat zur Folge, dass materiell verfassungswidrige Gesetze auch der EU-DSGVO widersprechen und umgekehrt. Enthalten die bereichsspezifischen nationalen Regelungen aber prozedurale oder organisatorische Normen, insbesondere hinsichtlich des Datenschutzmanagements bei den Verantwortlichen, der Selbstregulierung und der staatlichen Aufsicht, so kann insofern doch eine Anpassung an die EU-DSGVO erforderlich sein. Jedenfalls ist die Befürchtung, dass nach Inkrafttreten der Verordnung alle bereichsspezifischen Gesetze in Deutschland zur Randnotiz in der Datenschutzgeschichte würden, unbegründet.

Äußerst umstritten war Art. 6 Abs. 4, der die Voraussetzungen für *Zweckänderungen* regelt. Die Norm muss im Zusammenhang mit den Absätzen 1 und 2 gelesen werden, in denen allgemeine Voraussetzungen für rechtmäßige Datenverarbeitungen definiert werden. Zusätzlich werden Kriterien benannt, die bei einer Zweckänderung berücksichtigt werden müssen: a) die Verbindung des neuen mit dem ursprünglichen Zweck, b) der Erhebungszusammenhang, c) die Sensibilität der Daten, d) die möglichen Folgen der Weiterverarbeitung für die Betroffenen und e) angemessene Schutzmaßnahmen wie z. B. Verschlüsselung oder Pseudonymisierung.

7 Einwilligung

Die Einwilligung ist und bleibt eine zentrale Legitimation für die Datenverarbeitung (Art. 7). Die Diskussion über die Bedeutung, die Voraussetzungen und die Rahmenbedingungen von datenschutzrechtlichen Einwilligungen wird seit Jahren engagiert geführt. Diese Debatte findet mit der EU-DSGVO kein Ende, wohl erfolgen aber einige Konkretisierungen. Die allgemeinen Anforderungen an die Einwilligung ändern sich jedoch nicht: inhaltliche Bestimmtheit, Hervorhebungspflicht, Widerrufsmöglichkeit, Freiwilligkeit.

Konkretisierungen hinsichtlich der Einwilligungserfordernisse bestehen insofern, als die Einwilligung bzw. das Ersuchen danach „in verständlicher und leicht zugänglicher Form in einer klaren und einfachen Sprache“ zu erfolgen hat. Beim Widerruf dürfen keine formellen Hürden errichtet werden. In Art. 7 Abs. 4 wird unter dem Stichwort Freiwilligkeit ein eingegrenztes *Koppelungsverbot* normiert: Wird für einen Vertrag oder eine Dienstleistung eine Einwilligung abverlangt, „die für die Erfüllung des Vertrags nicht erforderlich ist“, so ist sie im Zweifel nicht freiwillig. Unklar sind die Rechtsfolgen einer unzulässigen Koppelung. Diese dürfte die Unzulässigkeit der gesamten Einwilligung zur Folge haben. In jedem Fall kann ein Widerruf der Einwilligung deren Wirkung für die Zukunft aufheben. Bei der Anwendung der Regelung kann es letztlich auch nicht darauf ankommen, ob eine Einwilligung als solche oder als Vertragsbestandteil bezeichnet wurde.

Die Autoren der EU-DSGVO legten sich nicht auf eine Altersgrenze für die Einwilligungsfähigkeit von *Kindern* bzw. Jugendlichen fest. In Deutschland wird bisher auf die Einsichtsfähigkeit abgestellt. Da hierüber in den nationalen Rechtskulturen unterschiedliche Vorstellungen herrschten und eine Einigung nicht möglich war, können die nationalen Gesetzgeber künftig zwischen vollendetem 13. und 16. Lebensjahr eigene Festlegungen vornehmen. Unter dieser Grenze muss bei einem Einwilligungsbedarf die Zustimmung der Eltern eingeholt werden. Es wird zudem klargestellt, dass die Einwilligung zur Datenverarbeitung und die sonstige Geschäftsfähigkeit getrennt voneinander zu beurteilen sind (Art. 8).

8 Besondere Datenkategorien

Hinsichtlich der Verarbeitung *sensitiver Daten*, also von Daten aus „besonderen Kategorien“, gibt es keine wesentlichen Änderungen: Einen besonderen Schutz gibt es auch in Zukunft für Daten zur rassischen und ethnischen Herkunft, zu politischen Meinungen, religiösen oder weltanschaulichen Überzeugung, Gewerkschaftszugehörigkeit, Gesundheit, Sexualleben und sexueller Ausrichtung. Eine Präzisierung erfolgt dadurch, dass in den Katalog die genetischen Daten sowie biometrische Daten zur eindeutigen Personenidentifizierung aufgenommen wurden (Art. 9). Trotz der zunehmenden Schutzbedürftigkeit von Finanztransaktionsdaten, die sich durch die zunehmende Digitalisierung des Zahlungsverkehrs und deren Bedeutung für Identitätsdiebstähle ergibt, wurde die

Kategorie nicht in den Schutzbereich der sensitiven Daten aufgenommen.

Die *Ausnahmen* von dem grundsätzlichen Verarbeitungsverbot erinnern an den bisherigen europäischen Regelungsrahmen. Als Ausnahme wird zunächst die explizite Einwilligung genannt. Es ist erfreulich, dass in begründeten Fällen spezialgesetzliche Einwilligungsverbote ausdrücklich zugelassen werden. In folgenden Fällen muss keine Einwilligung eingeholt werden: bei Ausübung von Rechten aus dem Arbeitsrecht, der sozialen Sicherheit und des Sozialschutzes, zum Schutz lebenswichtiger Interessen bei Einwilligungsunfähigkeit, bei der Verarbeitung durch einen sog. Tendenzbetrieb, bei vom Betroffenen offenkundig veröffentlichen Daten, zur Durchsetzung rechtlicher Ansprüche, zur Gesundheitsvorsorge, Arbeitsmedizin, medizinischen Diagnostik, zur Versorgung und Behandlung, zur Verwaltung im Gesundheits- und Sozialbereich, im öffentlichen Gesundheitswesen, für Archivzwecke, zur wissenschaftlichen und historischen Forschung und für statistische Belange.

Die gegenüber den bisherigen Erlaubnistatbeständen zur Verarbeitung sensitiver Daten vorgenommenen *Änderungen* sollen bisherige Regelungsdefizite beseitigen. So wird nicht mehr zwischen öffentlicher und privater Verwaltung von Systemen und Diensten im Gesundheits- und Sozialbereich unterschieden, so dass, anders als bisher, Privatversicherungen von der Ausnahmeregelung mit erfasst sein können.

Bzgl. der sensitiven Daten bestehen weitgehend nationale *gesetzliche Konkretisierungsmöglichkeiten*, wobei erhöhte Verarbeitungsvoraussetzungen nötig sein können. Damit kann das hochkomplexe Regelungsgeflecht beim Datenschutz im deutschen Sozialrecht weitgehend beibehalten werden. So sehr das von Seiten der Verantwortlichen begrüßt werden dürfte, so schade ist es, dass die EU-DSGVO nicht dazu zwingt, das unstrukturiert gewordene Datenschutzrecht in den Sozialgesetzbüchern I bis XII einer Totalrevision und Bereinigung zu unterwerfen.

In der Verordnung wird ein spezifisch (national) regelungsfähiger Aspekt explizit erwähnt: die Verarbeitung besonders sensibler Daten durch Fachpersonal, das z. B. einem besonderen *Berufsgeheimnis* unterliegt. Das vorliegende Regelungskonzept machte es überflüssig, nochmals gesondert die Verarbeitung für Gesundheitszwecke zu normieren, wie es zunächst von der Kommission in einem Art. 81 vorgesehen war (siehe aber Art. 90 zu Berufsgeheimnissen allgemein). Werden Berufsgeheimnisse nicht von den in Art. 9 genannten Tatbeständen erfasst, so muss im Einzelfall geprüft werden, ob die in § 203 StGB sowie in weiteren nationalen Spezialgesetzen enthaltenen Berufsgeheimnisse von nationalen Ausnahmeklauseln erfasst werden und ob eine Kollision zur EU-DSGVO entstanden ist.

Für Daten über *strafrechtliche Verurteilungen* und Straftaten oder damit zusammenhängende Sicherungsmaßregeln werden in Art. 10 spezifische Verarbeitungsvoraussetzungen benannt: Die Verarbeitung muss „unter behördlicher Aufsicht“ erfolgen; anderenfalls bedarf es angemessener gesetzlicher Garantien.

9 Betroffenenrechte

Die Rechte der Betroffenen und deren Beschränkungen sind in den Art. 12 bis 23 geregelt. Anders als bisher ist der Normierung der einzelnen Rechte ein *allgemeiner Teil* vorangestellt, in dem Adressatengerechtigkeit, Präzision, Transparenz, Verständlichkeit, leichte Zugänglichkeit und weitestgehende Unentgeltlichkeit eingefordert werden. Als Standard-Reaktionsfrist wird der verantwortlichen Stelle ein Monat vorgegeben (Art. 12).

Die meisten der normierten *Betroffenenrechte* sind bekannt: Information bei der Erhebung (Art. 12) bzw. Information, wenn die Daten nicht beim Betroffenen erhoben werden (Art. 14), Auskunft (Art. 15), Berichtigung (Art. 16), Löschung (Art. 17), Sperrung (Art. 18), was technisch präziser als „Einschränkung der Verarbeitung“ bezeichnet wird, Widerspruch generell (Art. 21) bzw. bei automatisierten Einzelentscheidungen (Art. 22) und der zu einem Nutzungsverbot für Werbezwecke führende spezifische Werbewiderspruch (Art. 21 Abs. 2 u. 3).

Gegenüber den bisherigen Regelungen gibt es einige kleine *Verbesserungen:* So wird klargestellt, dass zum Berichtigungsanspruch auch das Recht auf Vervollständigung unvollständiger Daten gehört. Der Löschanspruch wird mit dem schillernden Marketing-Begriff des „Rechts auf Vergessenwerden“ flankiert. Als Abwägungstopoi für den Löschungsanspruch werden die Rechte auf freie Meinungsäußerung und auf Information genannt.

Neu ist das Recht auf *Datenübertragbarkeit*. Dieses Recht bezieht sich auf Daten, die ein Wirtschaftsunternehmen vom Betroffenen auf der Basis eines Vertrages oder einer Einwilligung erhalten hat. Wenn die Verarbeitung automatisiert erfolgt, soll der Betroffene deren Bereitstellung in einer zu einem anderen Unternehmen übertragbaren Form verlangen können. Die Datenübertragung kann über den Betroffenen, aber wahlweise auch direkt zum neuen Diensteanbieter erfolgen (Art. 20). Wie dies in der Praxis umgesetzt werden soll, ist sowohl technisch als auch (außerhalb des Anwendungsbeispiels „soziale Netzwerke“) vom Umfang her noch weitgehend unklar.

Die Regelung zur automatisierten Einzelentscheidung wird mit dem Zusatz „einschließlich Profiling“ ergänzt. Letztlich wird versucht, damit einen Teilbereich so genannter *Big-Data-Auswertungen* zu regulieren. Da der Verordnungsgeber erkannt hat, dass ihm hierzu sowohl Erfahrung als auch das nötige differenzierende Instrumentarium fehlen, behilft er sich erneut mit einer Öffnungsregelung für die nationalen oder europäischen Normgeber. Um in diesem exorbitant wichtigen Feld aber die europarechtliche Kontrolle zu wahren, werden bei der Normierung „geeignete Maßnahmen zum Schutz der Rechte und Freiheiten“ gefordert. Problematisch an der Regelung bleibt, dass Big-Data-Anwendungen, die nicht auf „Entscheidungen“ hinauslaufen, ausdrücklich nicht erfasst werden. Bisher war streitig, ob die Entscheidung, jemandem auf Basis von Profiling Werbung zuzusenden, unter die Regelung zu automatisierten Entscheidungen fällt. Durch die Einbeziehung des Profiling kann herausgelesen werden, dass diese Streitfrage zumindest beim Einsatz dieser Methode, was auch immer genau darunter verstanden wird, zugunsten der Betroffenen zu beantworten ist.

Eine ungewöhnliche, aber angesichts der anscheinend bestehenden nationalen Unterschiede einzig konsensfähige Regelung wurde bei der Beschränkung der Betroffenenrechte gewählt: Während das Betroffenenrecht selbst sich direkt aus der Verordnung ergibt, werden die Einschränkungen national geregelt, wobei dem nationalen Gesetzgeber hierfür materielle Vorgaben gemacht werden. Dabei werden bekannte Abwägungsmuster benannt, vom „Schutz der nationalen Sicherheit" bis zum „Schutz der Rechte und Freiheiten anderer Personen" (Art. 23).

10 Verantwortlichkeit

Im Kapitel IV der Verordnung werden unter der Überschrift „Verantwortlicher und Auftragsdatenverarbeiter" verschiedene Aspekte geregelt, unter anderem auch, was bisher dem Begriff *„technisch-organisatorische Maßnahmen"* behandelt wurde. Die nun vorgelegten Regelungen gehen über das bisherige Verständnis teilweise weit hinaus. Die Verantwortlichkeiten nach der EU-DSGVO beschränken sich auch nicht auf dieses Kapitel, sondern erstrecken sich natürlich zudem auf die – an anderer Stelle geregelten – materiell-rechtlichen Pflichten wie z. B. die Erlaubnisregelungen und die Umsetzung der Betroffenenrechte.

Hinsichtlich der Datensicherheit wird, anders dies bisher explizit der Fall war, ein risikoorientierter Ansatz verfolgt. Dabei werden keine Schutzmaßnahmen aufgeführt, sondern die *Umsetzung von Datenschutzgrundsätzen* eingefordert, zu denen auch die Datenminimierung zählt (vgl. Ziffer 8). Als beschränkte Entlastung von Nachweispflichten wird die in Art. 42 normierte Zertifizierung erwähnt (Art. 25 Abs. 3).

Der *gemeinsamen Verantwortlichkeit mehrerer Stellen*, die begründet wird durch die gemeinsame Festlegung der Zwecke und Mittel der Datenverarbeitung, wird ein eigenständiger Artikel 26 gewidmet. Dabei wird, anders als bisher, eine „Vereinbarung in transparenter Form" gefordert, in der die Verantwortungsverteilung zu regeln ist. Fehlt eine Regelung, so hat dies für Betroffene keine nachteiligen Rechtsfolgen, da diese sich an jeden der Verantwortlichen wenden können. Angesichts der zunehmenden Arbeitsteilung bei der Datenverarbeitung, die oft nicht auf expliziten textlichen Vereinbarungen basiert, kann bezweifelt werden, ob mit der Regelung ein Fortschritt erreicht wird, der über die reine Benennung des Problems hinausgeht. Insofern hat der EuGH vom deutschen Bundesverwaltungsgericht (BVerwG) die Gelegenheit erhalten, eine dann auch für die EU-DSGVO geltende Interpretation vorzugeben, nachdem dieses dem EuGH am 25.02.2016 Fragen zur „Verantwortlichkeit" von Facebook-Fanpagebetreibern vorlegte.

Fehlt es in der EU an einer zur Verantwortung zu ziehenden Niederlassung, so muss gemäß Art. 27 ein in der EU ansässiger *„Vertreter"* benannt werden, der im Auftrag der verantwortlichen oder der auftragsdatenverarbeitenden Stelle bzgl. aller Datenschutzfragen als „Anlaufstelle" tätig wird.

Die *Verarbeitung im Auftrag* in Art. 28 hat einen über den heutigen § 11 BDSG hinausgehenden Detaillierungsgrad, ohne aber die darin enthaltenen Grundprinzipien in Frage zu stellen. Die gegenseitigen Hinweis- und Informationspflichten werden genauer benannt. So soll der Auftragsverarbeiter den Verantwortlichen präziser über Unterauftragsverhältnisse informieren. Unteraufträge müssen die gleiche Regelungstiefe aufweisen wie Aufträge. Es erfolgen Bezugnahmen zu genehmigten Zertifizierungen nach Art. 42 sowie genehmigten Standardvertragsklauseln. Es wird klargestellt, dass ein Auftragsverarbeiter, der auftragswidrig Zwecke und Mittel der Datenverarbeitung bestimmt, als Verantwortlicher zu behandeln ist.

Ein erklärtes Ziel der EU-DSVGO ist es, den bürokratischen Aufwand des Datenschutzes abzubauen. Dies soll aber nicht dazu führen, dass der für einen wirksamen Datenschutz nötige Aufwand nicht erbracht wird. Und nötig ist in jedem Fall der Überblick über die personenbezogene Datenverarbeitung für den Verantwortlichen bzw. Vertreter, weshalb diese weiterhin ein *Verfahrensverzeichnis*, genauer ein „Verzeichnis von Verarbeitungstätigkeiten" führen muss (Art. 30). Dies gilt auch für die Auftragsverarbeiter. Nicht verpflichtet werden Stellen mit weniger als 250 Beschäftigten, es sei denn, es bestehen besondere Verarbeitungsrisiken, etwa durch die Verarbeitung von besonderen Datenkategorien oder von Daten über Straftaten.

An die Stelle des technisch völlig überholten § 9 BDSG mit Anlage tritt hinsichtlich der *technisch-organisatorischen Maßnahmen* der Art. 30. Dieser fordert statt bestimmter Schutzmaßnahmen die Einhaltung der Schutzziele Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit und benennt als Instrumente u. a. die Pseudonymisierung und die Verschlüsselung. Warum ausgerechnet diese Maßnahmen durch explizite Nennung aus einer Vielzahl möglicher Maßnahmen herausgehoben werden und was unter „Belastbarkeit" zu verstehen ist, bleibt zunächst das Geheimnis des Gesetzgebers. Gefordert wird vor Durchführung einer Verarbeitung eine explizite Risikobewertung, ein darauf abgestimmtes Schutzkonzept sowie eine regelmäßige Evaluierung.

An die Stelle der bisherigen Vorabkontrolle tritt eine risikoorientierte *„Datenschutz-Folgeabschätzung"* bei spezifisch benannten Verfahren (systematische Personenbewertung, Verarbeitung sensibler Daten, Überwachung öffentlicher Räume) unter Einbeziehung eines möglicherweise vorhandenen Datenschutzbeauftragten (Art. 35). Es besteht die Pflicht zu einer *„vorherigen Konsultation"* der Datenschutzaufsichtsbehörde, wenn ein hohes Risiko besteht, sofern der „Verantwortliche keine Maßnahmen zur Eindämmung des Risikos trifft" (Art. 36).

In den Art. 33 und 34 ist die Meldung bzw. Benachrichtigung von Datenschutzverletzungen gegenüber der Aufsichtsbehörde sowie den Betroffenen (sog. *Breach Notification*) geregelt.

Entgegen der Befürchtung vieler deutscher Datenschützer sind in den Art. 37 bis 39 prominent die Benennung, die Stellung und die Aufgaben der (betrieblichen bzw. behördlichen) *Datenschutzbeauftragten* normiert und festgeschrieben. Die Pflicht zur Bestellung besteht bei öffentlichen Stellen, bei der „systematischen Beobachtung von betroffenen Personen" und bei der Verarbeitung sensibler Daten. Eine Bestellung kann national darüberhinausgehend verpflichtend gemacht werden, so dass der bestehende deutsche Regelungsrahmen beibehalten

werden kann. Die rechtliche Ausgestaltung des Datenschutzbeauftragten sowie dessen Aufgaben orientieren sich stark an den bisher geltenden deutschen Bestimmungen.

11 Regulierte Selbstregulierung

Das Instrument der *Verhaltensregeln* im privaten Bereich hat bisher nicht nur in Deutschland (§ 38a BDSG) wenig Resonanz gefunden. Das soll sich künftig dadurch ändern, dass deren Funktion und die Anreize hierfür erhöht werden (Art. 40, 41). So können hierüber für Kleinst- bzw. kleinere und mittlere Unternehmen Standardisierungen und damit Vereinfachungen vorgenommen werden. Über Verhaltensregeln können „geeignete Garantien“ festgelegt werden, die bei Datenübermittlungen in Drittländer innerhalb einer Branche verpflichtend sind. Die Regeln können und müssen eine „obligatorische Überwachung“ durch installierte Verbandsmechanismen z. B. in einer Branche vorsehen. Die Verhaltensregeln unterliegen, wie bisher, der Genehmigungspflicht durch die nach Art. 51 zuständige Aufsichtsbehörde und können von der EU-Kommission für verbindlich erklärt werden. Die Überwachung der Verhaltensregeln kann zu diesem Zweck akkreditierten Stellen übertragen werden (Art. 40). Durch die verbandsinterne Streitbeilegung können Verbände den Datenschutz also selbst in die Hand nehmen und dadurch zugleich die Aufsichtsbehörden entlasten.

Völlig neu ist auf europäischer Ebene die *Zertifizierung* gemäß den Art. 42, 43. Zertifizierungsverfahren, die freiwillig sind und transparent sein müssen, können von privaten Zertifizierungsstellen oder Aufsichtsbehörden durchgeführt werden. Unter anderem ist ein „Europäisches Datenschutzsiegel“ vorgesehen, für das der Europäische Datenschutzausschuss (EDA) Prüfkriterien festlegt. Private Zertifizierungsstellen bedürfen einer Akkreditierung durch die Aufsichtsbehörde oder durch eine nationale Akkreditierungsstelle, wobei die Voraussetzungen präzise in der Verordnung festgelegt sind. Zwecks Übersichtlichkeit werden alle anerkannten Zertifizierungsverfahren und Datenschutzsiegel in ein einheitliches Register aufgenommen. Sind die Voraussetzungen nicht (mehr) erfüllt, können sowohl Zertifizierungen als auch Akkreditierungen wieder entzogen werden. Die Kommission kann über Durchführungsakte technische Standards sowie Verfahrensvorgaben festlegen.

12 Auslandsdatentransfer

Hinsichtlich des *grenzüberschreitenden Datentransfers* ergeben sich gegenüber der Richtlinie keine grundsätzlichen Veränderungen. Wohl aber wurden viele Konkretisierungen vorgenommen, die insbesondere auch die Rechtsprechung des EuGH aufgreifen.

Innerhalb der EU gibt es keine spezifischen Übermittlungsbeschränkungen (Art. 1 Abs. 3). Gleiches gilt, wenn von der Kommission die *Angemessenheit des Datenschutzstandards* im Empfängerland festgestellt wurde. Für die Angemessenheitsprüfung enthält Art. 41 Abs. 2 einen umfangreichen Kriterienkatalog, der an die Kriterien des Safe-Harbor-Urteils des EuGHs anknüpft. Darin werden folgende Bedingungen genannt: Grundrechtsgeltung, auch im Bereich der öffentlichen Sicherheit, der Verteidigung und der nationalen Sicherheit, geltende Datenschutz-Rechtsvorschriften und unabhängige Datenschutzkontrolle. Eine Überprüfung ist alle 4 Jahre nötig.

Liegt kein genereller Angemessenheitsbeschluss der Kommission vor, so können an die Stelle staatlicher Datenschutzsicherungen im Empfängerland „geeignete Garantien“ treten, die bindend und durchsetzbar sein müssen. Als Beispiele werden nun ausdrücklich Standardvertragsklauseln und unternehmensinterne Datenschutzvorschriften (sog. Binding Corporate Rules – BCRs) genannt, aber auch genehmigte Verhaltensregeln oder Zertifizierungen (Art. 46). Für die Regelungen in BCRs werden in Art. 47 präzise Anforderungen festgelegt, zu denen die Umsetzung der Betroffenenrechte, die Haftungsübernahme im Fall von Verstößen, Beschwerde- und Konfliktlösungsverfahren und die Kooperation mit der Aufsichtsbehörde gehören. In einem neuen Artikel 48, der implizit auf US-Regelungen wie den Patriot Act Bezug nimmt, wird klargestellt, dass Drittlands-Gerichts- oder Verwaltungsentscheidungen nach europäischem Recht nur dann umgesetzt werden dürfen, wenn diese auf internationalen Abkommen basieren. Diese Regelung steht konzeptionell und inhaltlich im Konflikt mit dem Ende Februar 2016 vorgestellten EU-US Privacy Shield zur Datenübermittlung von Europa in die USA, das zu exekutiven und judikativen Entscheidungen führen wird, die nicht auf internationalen Abkommen beruhen.

Im *Einzelfall* können weiterhin Übermittlungen ohne allgemeine Garantien erfolgen, etwa bei ausdrücklicher Einwilligung, zur Vertragserfüllung, bei einem Betroffeneninteresse oder einem wichtigen öffentlichen Interesse, zur Durchsetzung von Rechtsansprüchen, zum Schutz lebenswichtiger Interessen oder in Rahmen einer Einzelentscheidung, die aber geeignete Garantien vorsehen muss.

13 Aufsichtsbehörden, Kooperation und Kohärenz

Dass es bisher massive Vollzugs- und Durchsetzungsdefizite im Datenschutz gibt, liegt u. a. daran, dass es keine verbindlichen Konfliktlösungsinstrumente zwischen den unabhängigen Datenschutzbehörden gab. So konnten z. B. Unternehmen in einem Land von der dortigen unzureichenden Datenschutzkontrolle profitieren. Dies wird durch Abstimmungszwänge in Zukunft erschwert. Hinsichtlich der Einrichtung, der Rechtsstellung und den Aufgaben der *Datenschutzbehörden* selbst wurde wenig geändert. Es erfolgen v. a. Konkretisierungen zur Unabhängigkeit (Art. 52), zur demokratischen Legitimation und fachlichen Qualifikation (Art. 43), zur Verschwiegenheit (Art. 54 Abs. 2), zur Zuständigkeit (Art. 55), zu den sehr umfassenden Aufgaben (Art. 57) und zu den ebenso äußerst umfassenden Befugnissen (Art. 58). Jeder Mitgliedstaat wird verpflichtet, die Aufsichtsbehörde bzw. -behörden mit den benötigten „personellen, technischen und finanziellen Ressourcen“ auszustatten (Art. 52 Abs. 4), was angesichts der gewachsenen Aufgaben bei den Behörden zu einer massiven Besserausstattung führen muss.

Neu ist die Etablierung einer auf ein Unternehmen bezogenen *federführen-*

den Aufsichtsbehörde, welche die wesentliche Datenschutzkommunikation mit einer verantwortlichen Stelle führt. Federführend ist die für die Hauptniederlassung in Europa zuständige Behörde. Diese ist nur dann nicht zwingend zuständig, wenn der konkrete Vorgang ausschließlich den Zuständigkeitsbereich einer anderen Aufsichtsbehörde betrifft. Aber auch in diesem Fall kann die federführende Behörde den Vorgang innerhalb einer Frist von drei Wochen an sich ziehen (Art. 56).

Handelt es sich um einen Vorgang, der mehrere Aufsichtsbehörden betrifft oder zieht die federführende Behörde den Fall an sich, so kommen die Regelungen zur *Zusammenarbeit* zur Anwendung (Art. 60). Dazu gehören die Amtshilfe für einzelne Fragestellungen oder Sachverhaltsermittlungen, wozu der angefragten Behörde regelmäßig nur ein Monat zur Verfügung steht (Art. 61), ein umfassender zweckdienlicher Informationsaustausch und die Vorlage eines Beschlussvorschlags durch die federführende Behörde. Hiergegen kann eine andere betroffene Behörde innerhalb von vier Wochen Einspruch einlegen. Wird dem nicht abgeholfen, erfolgt das Kohärenzverfahren. Wurde kein Einspruch eingelegt, so sind alle betroffenen Behörden an den Beschluss gebunden, der dann gegenüber der (Haupt-)Niederlassung ergeht und dem Beschwerdeführer mitgeteilt wird. Eine einheitliche Beschwerde kann in Teilbeschlüsse aufgeteilt werden. Für die Zusammenarbeit wird ein gemeinsames elektronisches Kommunikationsverfahren genutzt (Art. 67).

Eine besondere Form der Zusammenarbeit besteht in *gemeinsamen Maßnahmen* (Art. 62). Diese erfolgen, wenn Beschlüsse erhebliche Auswirkungen auf die Zuständigkeitsbereiche von mehreren Behörden haben werden. Hierzu lädt eine Aufsichtsbehörde ein; jede betroffene Behörde kann sich anschließen. Die teilnehmenden Behördenmitarbeiter erhalten dann Kompetenzen gemäß dem jeweils geltenden nationalen Recht.

Im *Kohärenzverfahren*, also bei unterschiedlichen Meinungen zu einem Beschlussvorschlag, wird die Stellungnahme des *Europäischen Datenschutzausschusses* (EDA) eingeholt. Außerdem kann jede Aufsichtsbehörde bei Angelegenheiten mit allgemeiner Geltung oder Auswirkungen eine solche Stellungnahme bewirken. Die Beschlussfassung erfolgt regelmäßig innerhalb von 8 Wochen mit einer einfachen Mehrheit der EDA-Mitglieder. Soweit erforderlich und zweckdienlich, werden Informationen übersetzt. Teilt eine Aufsichtsbehörde unter Angabe der maßgeblichen Gründe dem EDA mit, dass sie der EDA-Stellungnahme nicht folgt, so findet in einem weiteren Schritt eine Streitbeilegung durch den EDA statt (Art. 65). Diese erfolgt in Form eines innerhalb von einem Monat gefällten Beschlusses, für den eine 2/3-Mehrheit im EDA nötig ist. Die EDA-Beschlüsse werden auf der EDA-Webseite allgemein veröffentlicht.

Abweichend vom Kohärenzverfahren kann eine betroffene Aufsichtsbehörde ein *Dringlichkeitsverfahren* durchführen, durch das einstweilige Maßnahmen mit einer Geltungsdauer von höchstens 3 Monaten festgelegt werden (Art. 66).

Der Europäische Datenschutzausschuss besteht aus den Leitern der Aufsichtsbehörden, je einer pro Land. In Deutschland muss aus den föderalen Aufsichtsbehörden nach nationalen Regeln ein Behördenleiter benannt werden (Art. 68). Hauptaufgabe des EDA, dem eine eigene Rechtspersönlichkeit zukommt, ist die Abgabe von Stellungnahmen und die Beschlussfassung im Kohärenzverfahren. Daneben nennt Art. 70 viele weitere Aufgaben, u. a. die Beratung der Kommission, die Bereitstellung von Leitlinien, Empfehlungen und Verfahren, die Förderung von Verhaltensregeln und Zertifizierungsverfahren, die Akkreditierung von Zertifizierungsstellen, Stellungnahmen zum „angemessenen Schutzniveau", die Förderung der Zusammenarbeit zwischen den Aufsichtsbehörden, einschließlich Information und Schulung des Personals sowie die Öffentlichkeitsarbeit. Geleitet wird der EDA von einem Vorsitzenden und zwei Stellvertretern, die mit einfacher Mehrheit gewählt werden. Das EDA-Sekretariat wird beim Europäischen Datenschutzbeauftragten eingerichtet (Art. 75).

14 Rechtsschutz und Sanktionen

Bisher waren die national geregelten Rechtsschutz- und Sanktionsmöglichkeiten im Datenschutzrecht sehr begrenzt. Im Safe-Harbor-Urteil hatte der EuGH schon Nachbesserungen eingefordert. In diesem Bereich erfolgen in der EU-DSGVO nun sehr weitgehende Verbesserungen:

So haben *Betroffene* nicht nur gegenüber der Aufsichtsbehörde ein Beschwerderecht (Art. 77). Sie erhalten zudem eine gerichtliche Rechtsbehelfsmöglichkeit gegen eine sie betreffende rechtsverbindliche Entscheidung sowie auch, wenn eine Beschwerde nicht innerhalb von drei Monaten behandelt wurde; die abschließende Entscheidung darf längere Zeit in Anspruch nehmen (Art. 78). Ein Informationsanspruch besteht nicht nur zu den Verfahrensergebnissen, sondern auch zum Bearbeitungsstand. Mit dem neuen Instrument kann ein Betroffener eine materiell-rechtlich korrekte Entscheidung gegenüber der Aufsichtsbehörde einklagen, was bisher nicht anerkannt, geschweige denn effektiv realisiert war. Eine Rechtsschutzmöglichkeit besteht für den Betroffenen weiterhin – wie bisher – gegenüber der verantwortlichen Stelle oder dem Auftragsverarbeiter, wobei verbraucherfreundlich gegen private Verantwortliche die Klage im Mitgliedstaat des Betroffenen eingelegt werden kann.

Neu ist eine Art *Verbandsklage*, bei der eine Einrichtung, Organisation oder Vereinigung die Rechte des einzelnen oder von vielen Betroffenen gerichtlich geltend machen kann. Darüber hinaus besteht für die Mitgliedstaaten das Recht, unabhängig von Aufträgen von Betroffenen, Verbandsklagen zuzulassen (Art. 80). Entsprechendes erfolgte erst kürzlich in beschränktem Umfang in Deutschland.

Um in Europa divergierende Entscheidungen bei parallelen Verfahren zu vermeiden, kann ein zuständiges Gericht sein Verfahren aussetzen, wenn derselbe Gegenstand vor einem anderen Gericht innerhalb des Geltungsbereichs der Verordnung anhängig ist. Es erfolgt dann eine Abstimmung zwischen den Gerichten oder eine Zusammenführung der Verfahren (Art. 81).

Wie schon bisher (in Deutschland nur im privaten Bereich), haben die Aufsichtsbehörden die Möglichkeit, Warnungen und *Untersagungsverfügungen* zu erlassen (Art. 58 Abs. 2 lit. a-h, j).

Daneben sind Sanktionen in Form von empfindlichen Geldbußen möglich, die „in jedem Fall wirksam, verhältnismäßig und abschreckend“ sein müssen (Art. 83 Abs. 1). Dafür benennt die Verordnung eine Vielzahl von Sanktionszumessungskriterien, die es künftig ermöglichen, über Vergleiche europaweit eine Angleichung bzw. Harmonisierung zu erreichen. Abhängig vom Verstoß können Geldbußen bis zu einer Höhe von 10 Mio. €, in besonderen Fällen bis zu 20 Mio. € bzw. „im Fall von Unternehmen von bis zu 2 % (4%) seines gesamten weltweit erzielten Jahresumsatzes des vorangegangenen Geschäftsjahres“ verhängt werden. Ob und wenn ja, wie und in welchem Umfang Geldbußen bei Datenschutzverstößen durch öffentliche Stellen verhängt werden können, bleibt den Mitgliedstaaten überlassen (Art. 83 Abs. 7). Sieht die Verordnung für bestimmte Verstöße keine Sanktionen vor, so bleibt es den Mitgliedstaaten vorbehalten, auch diese zu sanktionieren (Art. 84).

15 Sonderregelungen

In einigen Bereichen überlässt der europäische Verordnungsgeber es den Mitgliedstaaten, *spezifische Regelungen* zu erlassen und macht hierfür Vorgaben. Dies gilt für die Datenverarbeitung „zu journalistischen Zwecken und zu wissenschaftlichen, künstlerischen oder literarischen Zwecken“ (Art. 85), für den Zugang der Öffentlichkeit zu amtlichen Dokumenten (Art. 86), die Verwendung einer nationalen Kennziffer (Art. 87), die Datenverarbeitung im Beschäftigtenkontext (Art. 88) und die Verarbeitung „zu im öffentlichen Interesse liegenden Archivzwecken, zu wissenschaftlichen und historischen Forschungszwecken und zu statistischen Zwecken“ (Art. 89).

Auf zunächst *geplante Sonderregelungen* zur Verarbeitung im öffentlichen Sektor generell, was die Bundesregierung lange gefordert hatte (Art. 80aa im Entwurf), sowie für Gesundheitszwecke (Art. 80b im Entwurf) wurde verzichtet, weil nationale Normierungsbefugnisse schon in die materiellen Regelungen (Art. 6 Abs. 3, Art. 9 Abs. 2, Art. 10) aufgenommen worden sind. Europäisch oder national geregelte (berufliche) Geheimhaltungspflichten können neben dem Datenschutzrecht weiterhin Anwendung finden. Dies betrifft in Deutschland beispielsweise den § 203 StGB und bereichsspezifische Konkretisierungen etwa im Anwalts-, Arzt- oder Notarrecht (Art. 90). Das in Deutschland geltende Kirchenprivileg zur Normierung des Datenschutzes soll weiterbestehen, soweit die Vorschriften „mit dieser Verordnung in Einklang gebracht werden“ (Art. 91).

Im Kommissionsentwurf war noch vorgesehen, dass die EU-Kommission eine Vielzahl von Befugnissen zum *Erlass delegierter Rechtsakte* erhält. Diese Möglichkeiten wurden weitgehend eingeschränkt, sind aber in einem gewissen Rahmen weiterhin vorgesehen (Art. 92).

In Art. 97 ist eine regelmäßige *Evaluation* der Verordnung vorgesehen, deren Ergebnis erstmals spätestens vier Jahre nach Inkrafttreten vorgelegt werden muss.

16 Ausblick

Die EU-DSGVO wird am 25.05.2018 in Kraft treten.

Der Anspruch der Verordnung, ein EU-weit einheitliches Datenschutzniveau festzulegen, wurde in vielen Bereichen nicht erreicht. Die EU-DSGVO enthält viele Öffnungsklauseln, durch die Mitgliedstaaten voneinander abweichende Regelungen erlaubt werden. Dieses Regelungskonzept war angesichts der bisher bestehenden, stark divergierenden nationalen Regelungen unvermeidbar. Viele Mitgliedstaaten forderten, bestimmte, aus ihrer Sicht bewährte Mechanismen beizubehalten. Dies gilt insbesondere auch für die Regierung Deutschlands, wo derzeit das europaweit wohl am stärksten ausdifferenzierte Datenschutzrecht besteht. Das Resultat, eine auch zukünftige begrenzte Heterogenität, war auch deshalb nicht zu vermeiden, weil differenziertere Regelungen den EU-Gesetzgeber zweifellos überfordert hätten.

Diese Heterogenität wird aber in keiner Weise zementiert. Eine *vereinheitlichende Wirkung* kann schon dadurch erreicht werden, dass durch diverse Meldepflichten gegenüber der Kommission ein Überblick über divergierende Regelungen verschafft wird. Da viele Öffnungsklauseln sich nicht nur an die nationalen, sondern auch an den EU-Gesetzgeber wenden, besteht die Aussicht, dass die EU weitere – bereichsspezifische – Regelungen erlässt.

Vorläufig ist es sehr wahrscheinlich, dass auslegungsbedürftige Regelungen in der Verordnung national oder gar regional von Anwendern, Aufsichtsbehörden und Gerichten unterschiedlich ausgelegt werden. Durch die Vorlagemöglichkeit beim EuGH nach Art. 267 AEUV sowie generell durch die Rechtsprechung des EuGH – etwa in Fällen des Art. 263 AEUV – kommt diesem Gericht auf lange Sicht eine wichtige, rechtsvereinheitlichende Funktion zu.

Die *deutschen Gesetzgeber* in Bund und Ländern – wie auch die der anderen Mitgliedsländer – sind aufgefordert, ihre bisherigen Datenschutzregelungen bis zum Inkrafttreten der Verordnung anzupassen. Dies bedeutet, dass das BDSG sowie die Landesdatenschutzgesetze zu Ausführungsgesetzen der EU-DSGVO umgestaltet werden müssen. Eine erste Meinungsbildung hierzu fand am 24.02.2016 im Ausschuss „Digitale Agenda“ des Deutschen Bundestags statt. So können unter Anknüpfung an die Verordnung nationale Besonderheiten bewahrt bleiben, wie z. B. die teilweise weitergehenden Regelungen zum betrieblichen Datenschutzbeauftragten in Deutschland. Dieser Pluralismus innerhalb der EU kann und sollte für einen europäischen Föderalismus befruchtend sein und den Wettbewerb um die besten Datenschutzinstrumente befördern. Bereichsspezifische Regelungen – vom Aufenthaltsgesetz bis zu den Statistikgesetzen – sind daraufhin zu überprüfen, ob sie weiterhin mit der EU-DSGVO vereinbar sind.

Die vielfältigen Öffnungsregelungen belassen den nationalen Gesetzgebern in den Mitgliedstaaten einen teilweise noch sehr weitgehenden Regelungsspielraum. Diese Öffnungsregelungen beschränken sich nicht darauf, die allgemeinen Regelungen der EU-DSGVO zu präzisieren. Nationale Gesetzgeber können durch innovative Gesetzgebung auch als Vorbild für andere Mitglieder der EU dienen und dadurch den digitalen Grundrechtsschutz voranbringen. Dies ist etwa im Bereich des Beschäftigtendatenschutzes möglich und wünschenswert. Innova-

tionsbedarf besteht aber nicht nur hier, sondern in praktisch allen Bereichen der personenbezogenen Datenverarbeitung.

Der EU ist mit der EU-DSGVO zweifellos ein fortschrittliches Regelwerk zum Datenschutz gelungen. Dieses hat aber weiterhin Defizite, die sich möglicherweise erst bei der Anwendung erweisen. Die technische, ökonomische und soziale Entwicklung fordert schon heute und laufend weitere Ergänzungen und Modifikationen, mit denen der digitale Grundrechtsschutz fortgeschrieben werden kann und muss. Der Ball liegt also nun wieder im Feld der nationalen Gesetzgeber, die auf der sicheren Rechtsgrundlage der aktuellen EU-DSGVO aufsetzen können und sollten.

Sabine Leutheusser-Schnarrenberger

Entscheidung des EuGH zum sog. Recht auf Vergessenwerden

Das Urteil des Europäischen Gerichtshofs (EuGH) vom 13. Mai 2014,[1] in dem das Gericht zwar nicht ausdrücklich, aber nach Meinung vieler Kommentatoren, ein „right to be forgotten“, ein sog. Recht auf Vergessenwerden, eingeführt hat, hat in die Diskussion der Verantwortlichkeit für im Internet verbreitete und zugänglich gemachte Inhalte eine neue Dimension gebracht.

Der EuGH hat der millionenfachen Verbreitung privater Informationen, auch wenn sie zutreffend sind, mit Hilfe des Datenschutzes und des Rechts auf Schutz der Privatsphäre einen begrenzt wirkenden Riegel vorgeschoben. Er verteilt die Verantwortung auf Beteiligte an der digitalen Kommunikation und hat deshalb den Suchmaschinenbetreibern, die eine Schlüsselstellung beim schnellen und leichten weltweiten Zugriff auf die gesuchten Informationen einnehmen, die Verpflichtung zur Löschung von Links unter bestimmten Voraussetzungen auferlegt. Der EuGH hat mit dieser Entscheidung Neuland betreten und sich institutionell neu positioniert.

Sachverhalt

Ausgangspunkt des beim Europäischen Gerichtshof durchgeführten Verfahrens war ein an die spanische Datenschutzbehörde AEPD (Agencia Espanola de Proteccion de Datos) gerichteter Antrag eines spanischen Klägers, Google-Spain zu verpflichten, einen bei namensbasierter Google-Suche in den Suchergebnissen enthaltenen Link zu einem 1998 erschienenen Artikel der spanischen Zeitschrift La Vanguardia zu löschen, in dem von einer Zwangsversteigerung einer dem Kläger gehörenden Immobilie bei Nennung des Klägernamens berichtet wurde. Die spanische Datenschutzbehörde AEPD hatte dem Antrag des Klägers stattgegeben und Google-Spain angewiesen, die erforderlichen Maßnahmen zu ergreifen, um die den Kläger betreffenden personenbezogenen Daten aus der Suchergebnisliste zu entfernen und den Zugang zu diesen Daten in Zukunft zu verhindern. Gegen diese Anweisung legte Google-Spain beim zuständigen spanischen Gericht, des Audiencia Nacional, Beschwerde ein, das seinerseits das Verfahren aussetzte und den Sachverhalt zur Vorabentscheidung dem Europäischen Gerichtshof vorlegte.

Die von dem spanischen Gericht dem EuGH zur Vorabentscheidung vorgelegten Fragen betreffen die Auslegung und die Anwendung der in der Europäischen Datenschutzrichtlinie 95/46/EG[2] enthaltenen Bestimmungen auf Internet-Suchmaschinen.

Aus der Begründung der Entscheidung ist ziemlich deutlich zu entnehmen, dass der Europäische Gerichtshof international agierende Konzerne für ihre Tätigkeit innerhalb der Europäischen Union zur Einhaltung europäischen Rechts verpflichten will. In Auslegung der europäischen Datenschutzrichtlinie hat der Gerichtshof damit bereits das Marktortprinzip entwickelt, das der europäische Gesetzgeber nunmehr in der Ende letzten Jahres verabschiedeten Datenschutzgrundverordnung[3], die mit Gültigwerden im Jahr 2018 die europäische Datenschutzrichtlinie ablösen wird, verankert hat.

Art. 17 der DS-GVO[4] setzt diese Entscheidung des EuGH um und begründet ein Recht auf Löschung der sie betreffenden personenbezogenen Daten gegenüber dem Verantwortlichen in unterschiedlichen Fallkonstellationen, zu denen u.a. gehört, wenn der ursprüngliche Zweck nicht mehr besteht (Art. 17 Abs. 1 a), die Einwilligung widerrufen worden ist oder wenn eine Rechtsgrundlage für die Verarbeitung fehlt (Art. 17 Abs. 1 b), oder wenn bei Widerspruch gegen die Verarbeitung keine vorrangigen berechtigten Gründe für die Verarbeitung vorliegen (Art. 17 Abs. 1 c).

Damit entfällt die frühere juristische Argumentation, mangels Sitz in der EU gelte das „strenge“ europäische Datenschutzrecht nicht. Und es wird der beliebten Praxis der internationalen IT-Konzerne ein Riegel vorgeschoben, mit der Sitzwahl eines Konzerns in der EU sich das auf niedrigstem Niveau bewegende Datenschutzrecht eines EU-Mitgliedstaates auszusuchen. Es wird künftig datenschutzrechtlich nichts mehr bringen, sich in Dublin anzusiedeln, wie das derzeit Facebook, Google und viele andere internationale Konzerne tun.

Löschungspflichten

Die Löschungspflichten des Suchmaschinenbetreibers betreffen jede von der Verarbeitung ihrer Daten betroffene Person, die von dem für die Verarbeitung Verantwortlichen „je nach Fall eine Berichtigung, Löschung oder Sperrung" der Daten verlangen kann, wenn die Verarbeitung nicht den Bestimmungen der Richtlinie entspricht, insbesondere wenn sie unvollständig oder unrichtig ist.[5]

Die Verarbeitung der Daten entspricht nicht nur dann nicht der Richtlinie, wenn diese sachlich unrichtig sind, sondern u. a. auch dann, wenn sie den Zwecken der Verarbeitung nicht entsprechen, dafür nicht erheblich sind, darüber hinausgehen, nicht auf dem neuesten Stand sind oder länger als erforderlich aufbewahrt werden, es sei denn, ihre Aufbewahrung ist für historische, statistische oder wissenschaftliche Zwecke erforderlich.

Die Pflicht zur Löschung entfällt jedoch dann, wenn sich aus besonderen Gründen – wie die Rolle der betroffenen Person im öffentlichen Leben – ergibt, dass der Eingriff in die Grundrechte der Person durch ein überwiegendes öffentliches Interesse daran, über die Einbeziehung in die Suchmaschinen-Ergebnisliste Zugang zu den enthaltenen Informationen zu haben, gerechtfertigt ist.[6]

Es sollen also gerade nicht Prominente und öffentliche Personen der Zeitgeschichte in die Lage versetzt werden, ihre Lebensläufe und ihr Wirken korrigieren zu können. Was unliebsam ist und nicht mehr in die politische oder wirtschaftliche Agenda passt, soll nicht durch Löschen der Links dem einfachen Zugriff entzogen werden.

Dieser Ansatz greift die zur Meinungs- und Äußerungsfreiheit entwickelten Grundsätze der Rechtsprechung auf. Die im Spannungsfeld stehenden Grundrechte der informationellen Selbstbestimmung, des Schutzes der Privatsphäre und der eigenen Persönlichkeit auf der einen Seite und der Meinungs- und Pressefreiheit auf der anderen Seite sind durch höchstrichterliche Rechtsprechung sorgfältig austariert worden. Das berechtigte Interesse der Öffentlichkeit an Informationen schränkt danach unter bestimmten Voraussetzungen den Persönlichkeitsrechtsschutz ein.

Kritik an dieser Entscheidung des EuGH wird aus dem Vorwurf der unzureichenden Abwägung mit dem Recht der Meinungs- und Äußerungsfreiheitfreiheit hergeleitet.[7]

Der EuGH habe in seiner Entscheidung der Bedeutung dieses für die Demokratie konstitutiven Grundrechts zu wenig Bedeutung beigemessen. Wenn nur noch von der Perspektive des Rechts auf informationelle Selbstbestimmung her gedacht werde, würde das an die Tradition der Aufklärung anknüpfende individuelle Recht auf freie Meinungsäußerung, das nicht unter einem wie auch immer gearteten Vorbehalt des öffentlichen Interesses stehe, im Kern geschwächt.

Diese Kritik, die nicht leichtfertig abgetan werden darf, verkennt jedoch, dass der EuGH sich in dieser Entscheidung nicht mit der Löschung der presserechtlichen Veröffentlichung befasst, sondern mit dem Zugang zu Presseartikeln und anderen online Publikationen mittels einer namensbasierten Recherche durch eine Suchmaschine. Der Artikel selbst bleibt bestehen und wird nur etwas schwieriger auffindbar. Deshalb handelt es sich eher um ein Recht des Betroffenen, sich besser dem öffentlichen Zugriff entziehen zu können.

Zwei Grundsätze für den Löschungsanspruch

Die Entscheidung enthält keinen ausführlichen Kriterienkatalog für die Löschung, was angesichts des einfachen zugrunde liegenden Sachverhalts auch nicht geboten war.

Zwei Grundsätze sind hervorzuheben:

1. Wirtschaftliche Interessen der Suchmaschinenbetreiber haben bei diesen Löschanträgen generell keinen Vorrang.

Die digitale Kommunikation verschiebt zwar die Abgrenzung zwischen privat und öffentlich, aber der Schutz der eigenen Daten und der Privatsphäre werden und dürfen nicht aufgegeben werden. Ihm wird vom EuGH ein grundsätzlicher Vorrang vor den wirtschaftlichen Interessen der Suchmaschinenbetreiber eingeräumt, es sei denn, es liegt ein überwiegendes öffentliches Interesse an dem Zugang zu diesen Daten durch namensbasierte Recherche vor. Damit muss eine Abwägung zwischen dem berechtigten Schutz des Datenschutzsubjekts an einer zweckgebundenen Verwendung seiner Daten und dem Interesse der Öffentlichkeit an Information stattfinden.

Festzuhalten ist, dass nicht die mit teilweise marktbeherrschender Stellung agierenden IT-Konzerne die uneingeschränkte Definitionshoheit darüber haben, was von ihnen an vorgegebenen Informationen verarbeitet und verbreitet wird, sondern dass sie an die europäisch geltenden Grundrechte gebunden sind.

2. Der Antragsteller darf nicht darauf verwiesen werden, zuerst gegen die Journalisten und deren Verlag wegen Verletzung des Persönlichkeitsrechts und des Datenschutzrechtes durch die Publikation vorzugehen. Die Ansprüche auf Delisting gegen die Suchmaschinenbetreiber und auf mögliche inhaltliche Korrektur gegen die Contentverantwortlichen bestehen nebeneinander und haben auch unterschiedliche Voraussetzungen. Sie sind nicht inhaltlich voneinander abhängig, denn auch **rechtmäßige** frühere Berichterstattung kann nach der Entscheidung des EuGH zu einem berechtigten Löschantrag führen.

An dieser Stelle nimmt der europäische Gesetzgeber eine Einschränkung vor. Nach Art. 17 Abs. 1 d DS-GVO besteht nur bei **unrechtmäßiger** Verarbeitung der personenbezogenen Daten ein Löschungsanspruch. Damit soll wohl Problemen begegnet werden, die in einem Auseinanderfallen der Rechtsprechung zum Äußerungsrecht in Abwägung mit dem Persönlichkeitsrechtsschutz und dem Datenschutzrecht liegen können. Keine ausdrückliche Regelung ist damit zu der Frage getroffen worden, in der nach einer rechtmäßigen Erfassung und Verarbeitung der Daten sich durch Zeitablauf ein anderer Sachverhalt ergeben hat und die ursprüngliche rechtmäßige Erfassung aktuell mit der tatsächlichen Situation nicht in Einklang zu bringen ist. Genau darum ging es ja in der Entscheidung des EuGH. Ein im Jahr 1998 insolventer Unternehmer wurde Jahre später wieder solvent und sollte in Zukunft davor geschützt werden, bei einer Recherche mit seinem Namen immer wieder mit Insolvenz in Verbindung gebracht zu werden. Bei

noch sensibleren Daten wie zum Beispiel der sexuellen Orientierung und der Veränderung des Geschlechts ist das Persönlichkeitsrecht des Betroffenen noch stärker berührt. Ob in diesen Fällen ein Anspruch gegen den Contentverantwortlichen auf Streichung der personenbezogenen Angaben wegen Verletzung des Persönlichkeitsrechtes besteht und auch durchgesetzt werden kann, kommt auf die Situation im Einzelfall an. Gerade diesen Problemen wollte der EuGH mit seiner Argumentation, dass unabhängig von der Rechtmäßigkeit der Ersterfassung ein Löschungsanspruch bestehen soll, wenn die Angaben „inadäquat, irrelevant, no longer relevant or excessive“ sind,[8] begegnen und begründete auch damit die Verantwortlichkeit der Suchmaschinenbetreiber. Es bleibt abzuwarten, wie sich nach Inkrafttreten der DS-GVO die Entscheidungspraxis der Suchmaschinenbetreiber und damit besonders von Google entwickeln wird.

Art. 17 DS-GVO enthält auch keinen abschließenden oder beispielhaft aufgeführten Kriterienkatalog für den Löschungsanspruch, so dass es auf die Gesamtbewertung des Sachverhalts ankommt, aber auch die Entscheidung des EuGH berücksichtigt werden muss.

Danach steht am Beginn der Entscheidungsfindung die Frage, ob es sich bei der betroffenen Person um eine Person des öffentlichen Lebens handelt, also um eine absolute oder relative Person der Zeitgeschichte oder um eine Privatperson. Das ist die erste Weichenstellung, denn bei Bejahung dieses Kriteriums wird die Abwägung in Richtung Ablehnung eines Löschbegehrens gestellt. Bei der Abwägung spielt auch eine Rolle ob der Antragsteller die Information selbst preis gegeben hat und damit sein Einverständnis erklärt haben kann und die Seriosität der Quelle.

Welche Rolle künftig der Zeitfaktor beim Löschungsanspruch spielen wird, ist angesichts der Anforderung der Unrechtmäßigkeit der Datenerfassung neu zu bewerten. Die einfache Formel, dass je weiter eine Berichterstattung zeitlich zurückliegt, das Löschbegehren umso berechtigter ist, wird nicht mehr greifen.

Verfahren

Der Suchmaschinenbetreiber, in diesem Fall Google, entscheidet allein über den Löschungsantrag. An dieser Rolle von Google entzünden sich viele Diskussionen. Die Bedenken richten sich gegen die starke Stellung, die Google damit erlangen würde. Außerdem könne der Gegner des Löschungsanspruchs nicht auch Entscheider sein. Diese Argumentation lässt unberücksichtigt, dass es in einem zivilrechtlichen Verfahren dem Anspruchsgegner nicht verwehrt werden kann, dem Begehren stattzugeben oder es abzulehnen. Man kann auch nicht Google datenschutzrechtlich in die Pflicht nehmen und sich dann darüber beklagen, wenn das Unternehmen dieser Verpflichtung nachkommt. Der Entscheidung muss aber eine fundierte Abwägung über die im Spannungsverhältnis stehenden Grundrechte zu Grunde liegen.

In diesem Kontext spielen Verfahrensregeln eine Rolle, die dem Inhaltsverantwortlichen Gelegenheit zur Stellungnahme vor der Entscheidung geben und ihm eine Beteiligtenstellung einräumen würden.

Das war die Haltung des Google Beirats zum sog. Recht auf Vergessenwerden, der im Juni 2014 von Google eingerichtet wurde und mit einem Bericht Empfehlungen zur Umsetzung des Urteils des EuGH erarbeitet hat.[9]

In Art. 19 der europäischen Datenschutz-Grundverordnung[10] sind nun Mitteilungspflichten der Verantwortlichen der Datenverarbeitung an alle Empfänger, denen personenbezogene Daten offengelegt wurden, im Fall der Löschung oder Beschränkung vorgesehen, es sei denn, der Aufwand wäre unverhältnismäßig oder die Mitteilung erweist sich als unmöglich. Und weitergehend wird auch den Verantwortlichen, die diese personenbezogenen Daten erst öffentlich gemacht haben, also auch den Contentverantwortlichen im Sinne des Äußerungsrechts, die Verpflichtung auferlegt, dies den Datenverarbeitern, also auch den Suchmaschinenbetreibern, mitzuteilen und sie zur Löschung der Links zu den Artikeln aufzufordern. Das soll dem sog. Recht auf Vergessen im Netz größere Geltung verschaffen (Art. 19 Abs. 2 DS-GVO). Das bedeutet letztendlich, dass nicht nur der Betroffene der personenbezogenen Datenerfassung und -verarbeitung einen Löschungsanspruch gegen den Vermittler hat, sondern alle Beteiligten in die Pflicht genommen werden.

Reichweite der Löschungsentscheidung

Zur Reichweite des Löschungsbegehrens gibt es auch in der DS-GVO keine Regelung. Dies ist derzeit ein weiterer Streitpunkt und wurde auch im Google Beirat unterschiedlich gesehen. Die EuGH-Entscheidung befasst sich mangels Begehr nicht damit, ob nur europäische Domains oder weltweit alle Domains gelöscht werden müssen. Es ging in der Entscheidung nur um die Löschung der spanischen Domain. Aber was bringt ein erfolgreicher Löschantrag in Spanien, wenn der betroffene Artikel von Deutschland, Frankreich oder anderen europäischen Mitgliedstaaten aus unter Benutzung des Namens gefunden werden kann? Nach Auffassung des Google Beirates müssen in jedem Fall alle europäischen Domains entfernt werden.

Das war dennoch bisher nicht die Praxis von Google. Auf Grund eines Verfahrens in Frankreich hat Google seine Praxis ändern müssen.

Google wird unter anderem die IP nutzen, um das „Aufrufs“-Land zu bestimmen. Nach Mitteilung von Google funktioniert das dann wie folgt: Stellt jemand einen erfolgreichen Antrag aus einem Mitgliedstaat der EU und wird dieser genehmigt, werden Suchergebnisse diesen Inhalt in diesem Land nicht mehr anzeigen, egal ob von der Google-Landesdomain aus gesucht wird oder über die Domain eines anderen Landes. Außerhalb des Landes ist der Inhalt wiederum über alle Google-Domains auffindbar. Wie Google mit VPN-Diensten umgeht, ist damit nicht ganz klar, da die Landeskennung nicht anhand der IP möglich ist, aber vielleicht ist die IP nur als Beispiel für die Erfassung des Standortes genannt.

Die Suche außerhalb der Länder bringt weiterhin alle Suchergebnisse hervor. Die Suche mittels Google.com zeigt weiterhin alle Suchergebnisse an. Angeblich würden nur 5% aller Suchanfragen aus Europa über Google.com durchgeführt.

Genau daran entzündete sich auch die kontroverse Debatte im Google Beirat.

Nach meiner Auffassung und der der Datenschutzexperten in Deutschland und in der Art. 29 Data Protection Working Party[11] kann bei einem globalen Internet ein wirkungsvoller Schutz auch nur mit globalem, also weltweiten Delisting der Links, also z.B. auch in den USA erreicht werden. Das lehnte Google ab. Jetzt hat vor kurzem Google seine Praxis noch einmal geändert. Mittels Geoblocking[12] will Google verhindern, dass europäische Nutzer über Google.com Suchergebnisse erhalten, die aus Datenschutzgründen auf den nationalen Seiten des Konzerns in Europa ausgeblendet werden. Damit versucht Google, eine Lücke bei der Handhabung des Urteils des EuGH zu schließen.

Praxis von Google

Nachdem Google zunächst die Entscheidung stark kritisiert hatte, hat sich das Unternehmen jetzt den Gegebenheiten gestellt und seine Infrastruktur in den Mitgliedstaaten entsprechend angepasst.

Es sind insgesamt in der EU seit dem 14. Mai 2014 ca 400.000 (398.244) Anträge auf Löschung eines Links zu Artikeln mit der Namensnennung des Antragstellers eingegangen, die europaweit über 1.401.670 URLs betreffen, davon in Deutschland mit ca 68.600 (249.000 URLs) die zweitmeisten nach Frankreich (ca 85.000, 280.608 URLs). Durchschnittlich werden europaweit ca 43% der Anträge (508.300 URLs) gelöscht und 57% der Anträge (684.300 URLs).

Das hört sich viel an, ist mit Blick auf 500 Mio. Bürgerinnen und Bürger der EU aber doch nicht so umfangreich wie in den ersten Wochen nach der Entscheidung befürchtet worden war.

Da über die Löschanträge bei anderen Suchmaschinenbetreibern (z.B. Microsoft) keine Statistik vorliegt, ist die Summe aller Anträge nicht bekannt.

Fazit

Die bedeutende Entscheidung des EuGH zur Verantwortlichkeit der Zugangsvermittler stärkt das Datenschutzrecht des Nutzers. Dies bezwecken auch die Regelungen in der europäischen Datenschutzgrundverordnung zum sog. Recht auf Vergessen. Welche Auswirkungen sie haben werden und wie sich die rechtliche und technische Praxis entwickeln wird, bleibt abzuwarten.

1 Urteil des Gerichtshofs vom 13. Mai 2014, Rechtssache C-131/12

2 Richtlinie 95/46/EG des Europäischen Parlaments und des Rates zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum Schutz des freien Datenverkehrs vom 24. Oktober 1995

3 Rat der EU, Brüssel 6. April 2016, 5419/16, Verordnung zum Schutz natürlicher Personen..., Datenschutz-Grundverordnung

4 a.a.O. unter 3, Seite 140

5 GH, a.a.O. FN 38, Ziffer 70

6 GH. a.a.O., Ziffer 97

7 Prof. Dr. Kai von Lewinski, Staat als Zensurhelfer – Staatliche Flankierung der Löschpflichten Privater nach dem Google-Urteil des EuGH, AfP 2015, 1ff

8 EuGH a.a.O., Ziffer 94

9 Report des Google Advisory Council, www.google.com

10 a.a.O., Seite 143

11 88. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 8. und 9. Oktober 2014 in Hamburg, Article 29 Data Protection Working Party 14/EN WP 225 vom 26. November 2014

12 http://www.heise.de/newsticker/meldung/Google-setzt-Recht-auf-Vergessen-in-der-EU-schaerfer-durch-3098801.html?view=print

Dr. Robert Selk

EU-DS-GVO: Neue Anforderungen an die Einwilligung?

Am 05.05.2016 wurde die EU-DS-GVO nunmehr im EU-Amtsblatt veröffentlicht und tritt damit 20 Tage später in Kraft. Wirkung entfaltet sie allerdings erst 24 Monate später, also zum 25.05.2018. Damit liegt die finale Fassung der EU-DS-GVO vor, die Einwilligung als eine Möglichkeit, eine Datenverarbeitung zu legitimieren, spielt weiterhin eine wichtige Rolle. Rund um die Einwilligung stellen sich eine Reihe von Fragen, insbesondere dazu, was sich aus deutscher Sicht ändert oder gleich bleibt. Dies betrifft z.B. die formalen Anforderungen oder die Thematik der Freiwilligkeit. Daneben ist eine sehr wichtige Frage, was mit „Alt-Einwilligungen" nach dem BDSG passiert: Bleiben diese auch nach dem 25.05.2018 wirksam? Oder müssen sie neu eingeholt werden? Der Beitrag gibt einen Überblick über die Änderungen und wirft einen Blick auf die Frage eines etwaigen Bestandsschutzes.

Einleitend: Zur Bedeutung der Einwilligung in der EU-DS-GVO

Bevor ein Blick auf die Änderungen zu werfen ist, bleibt festzuhalten, dass das bisherige datenschutzrechtliche Verbotsprinzip auch in der EU-DS-GVO bestehen bleibt: Danach ist jede Verarbeitung von personenbezogenen Daten verboten, soweit nicht entweder über eine gesetzliche Datenverarbeitungserlaubnis gestattet oder – wenn es keine

gesetzliche Erlaubnis gibt – über eine vom Betroffenen erteilte Einwilligung legitimiert ist, die die gewünschte Datenverarbeitung umfasst. Liegt weder eine gesetzliche Erlaubnis noch eine Einwilligung vor, ist die gewünschte Datenverarbeitung unzulässig.

Damit kommt der Einwilligung als eines der beiden Legitimationsmittel unverändert hohe Bedeutung zu. Dies gilt umso mehr, als dass der Einzelne es gerade über eine Einwilligung selbst in der Hand hat, zu bestimmen, was andere Stellen, wie etwa Firmen, über ihn wissen und mit „seinen" Daten an Verarbeitung durchführen dürfen.

Wo finden sich Regelungen zur Einwilligung in der EU-DS-GVO?

In der EU-DS-GVO finden sich die Regelungen zur Einwilligung in nur einem Artikel, nämlich Art. 7 EU-DS-GVO. Dies erscheint relativ knapp, betrachtet man die zentrale Rolle, die der Einwilligung zukommt.

Der EU-DS-GVO sind aber sehr umfänglich sog. Erwägungsgründe vorangestellt, in denen der europäische Gesetzgeber seine Gedanken und „Erwägungen" zusammengefasst darstellt. Dabei gilt die Besonderheit, dass die Erwägungsgründe Teil des europäischen Gesetzes, hier also der EU-DS-GVO und damit ebenso rechtswirksam sind. Mit anderen Worten: Die Erwägungsgründe müssen jeweils „mitgelesen" und bei der Auslegung der einzelnen Artikel beachtet werden. Zur Einwilligung finden sich in einigen Erwägungsgründen sogar ausführliche Hinweise, die zu einer Reihe von praxisrelevanten Fragen Informationen enthalten. Es sind insbesondere die Erwägungsgründe Nr. 32, 42, 43 und – was die Frage des Bestandsschutzes angeht – Nr. 171.

Was ändert sich also bei den Einwilligungen?

Das deutsche BDSG ist sehr streng, was die Anforderungen und Vorgaben an eine wirksame Einwilligung angeht, zum Teil strenger als die EU-Datenschutz-Richtlinie von 1995. Insofern liegen aus deutscher Sicht bei den Neuregelungen der EU-DS-GVO die Änderungen eher im Detail als in großen oder besonders auffälligen Punkten oder Themen. Im folgenden ein Überblick zu den wichtigsten Punkten, was sich (nicht) ändert:

Keine Schriftform mehr!

Eine Neuerung, die von erheblicher praktischer Bedeutung sein wird, ist der Umstand, dass eine Datenschutz-Einwilligung nach der EU-DS-GVO nicht schriftlich abgegeben werden muss.

Das BDSG schreibt in § 4 a Abs. 1 BDSG dagegen die Schriftform vor, nur wenn wegen „besonderer Umstände" eine andere Form „angemessen" ist, darf davon ausnahmsweise abgewichen werden. In besonderen Eilfällen etwa kann diese Ausnahme greifen. Da aber die Beweislast dafür, ob solche besonderen Umstände vorliegen, bei der verantwortlichen Stelle liegt, besteht bei dieser Frage in Deutschland in der Praxis oft erhebliche Rechtsunsicherheit: Ist etwa eine telefonisch einem Call Center gegenüber erteilte Einwilligung wirksam? Auch dann, wenn keine Eilsituation vorliegt?

Das deutsche Recht kennt zudem eine Art elektronische Form, die aber nur bei speziellen Daten im Internetbereich (sog. Bestands- und Nutzungsdaten) oder die Werbung betreffende Einwilligungen greifen kann; für alle anderen Formen von Einwilligungen gibt es in Deutschland keine elektronische Form.

Mit der EU-DS-GVO stellen sich diese Fragen dann nicht mehr, weil sie die „Grundanforderung" der Schriftlichkeit nicht kennt. Aus praktischer Sicht ist dies eine Erleichterung für beide Seiten, es entspricht auch der Digitalisierung und dem Wunsch, einen Medienbruch zu vermeiden und gewisse Dinge zu erleichtern (neben dem klassischen Datenschutz ist die Erleichterung und die Förderung des Datenverkehrs innerhalb der EU das zweite große Ziel der EU-DS-GVO).

Zugleich geht damit die der Schriftform innewohnende Warnfunktion verloren. Um dem zu begegnen, hat der europäische Gesetzgeber aber andere, zum Teil auch nur klarstellende Regelungen in der EU-DS-GVO aufgenommen.

Beweislast beim Verantwortlichen

So wird betont, dass die Beweislast dafür, dass der Betroffene auch tatsächlich eine (ausreichende) Einwilligung erteilt hat, bei der verantwortlichen Stelle liegt, also dem Unternehmen, das um die Einwilligung bittet. Aus deutscher Sicht ist dies nichts Neues, nunmehr aber gesetzlich geregelt (Art. 7 Abs. 1 EU-DS-GVO).

Alleine schon deswegen und in Anbetracht der sehr deutlich erhöhten Strafen bei Datenschutzverstößen ist man als Unternehmen gut beraten, möglichst umfassend dokumentiert Einwilligungen einzuholen. Dies kann ab 2018 aber auch in elektronischer Form oder per Scan o.Ä. erfolgen, eine Originalunterschrift ist dann nicht mehr nötig.

Hervorhebungspflicht

Dies führt zum nächsten Punkt, mit dem vermieden werden soll, dass Einwilligungen den Betroffenen „untergejubelt" werden, etwa als Teil von Allgemeinen Geschäftsbedingungen: Dazu regelt die EU-DS-GVO, dass eine Einwilligung, die Teil eines „größeren" Dokuments ist, das auch noch andere Inhalte aufweist (wie etwa AGB), dort von den anderen Sachverhalten klar zu unterscheiden sein muss. Mit anderen Worten: Wenn die Einwilligung Teil von AGB sein soll, muss sie dort optisch besonders hervorgehoben werden.

Auch dies ist aber nicht neu, das deutsche Recht kennt dazu schon explizite Regelungen im BDSG und das schon seit vielen Jahren. Umso erstaunlicher ist es, dass dies bis heute oft missachtet wird.

Neu dagegen ist die ausdrückliche Regelung in der EU-DS-GVO, dass das „Ersuchen um eine Einwilligung" in solchen Fällen in „verständlicher und leicht zugänglicher Form in einer klaren und einfachen Sprachen zu erfolgen hat". Inhaltlich dagegen handelt es sich um einen ohnehin geltenden Rechtsgrundsatz, der sich zudem auch noch aus dem AGB-Recht ergibt.

Was an einer Einwilligung ist bei einem Verstoß gegen die Vorgaben unwirksam?

Wichtig für die Praxis ist dagegen die nunmehr in der EU-DS-GVO aufgenommene ausdrückliche Regelung, dass nur diejenigen Teile einer Einwilligung unwirksam sind, die gegen die Rege-

lungen der EU-DS-GVO verstoßen. Mit anderen Worten: Die Regelungen, die in Ordnung sind, bleiben gültig.

Zugleich ist es so, dass die ungültigen, weil gegen die Verordnung verstoßenden Teile dann gänzlich entfallen: Es gibt damit keine Reduktion auf dasjenige, was man (gerade) noch hätte zulässigerweise regeln können. Grund dafür ist, dass man ansonsten einfach immer versuchen würde, das Maximale an Einwilligung „herauszuholen" und das Schlimmste, was bei einem Verstoß passieren würde, wäre, dass „nur" das gilt, was per Gesetz noch erlaubt ist. Auch diesen Rechtsgrundsatz kennt das deutsche Recht schon sehr lange im AGB-Recht.

Wie freiwillig muss eine Einwilligung sein?

Unverändert wichtig ist, dass eine Einwilligung freiwillig erteilt wird. Dies ist eine in der Praxis sehr wichtige Frage, da mit der Freiwilligkeit die Wirksamkeit der Einwilligung steht und fällt. In der EU-DS-GVO sind in Art. 7 Abs. 4 Aspekte genannt, die bei der Beurteilung der Freiwilligkeit zu berücksichtigen sind. Insbesondere soll danach eine Rolle spielen, ob ein Vertragsschluss etwa nur möglich ist, wenn der Kunde zugleich in der (meist werblichen) Verarbeitung derjenigen seiner Daten einwilligt, die nicht zur Vertragsdurchführung erforderlich sind.

Etwas strenger und damit gewissermaßen im Widerspruch dazu ist Erwägungsgrund Nr. 43, der bei solchen Koppelungen sogar von einer Unwirksamkeit spricht (was nach anderen rechtlichen Gründen etwas fragwürdig erscheint, da eine Einwilligung für Vorgänge, die schon zur Vertragsdurchführung erforderlich sind, nicht nötig ist). Es wird abzuwarten bleiben, welche Auswirkung dieser Erwägungsgrund genau auf die etwas weitere Regelung in Art. 7 EU-DS-GVO haben wird.

Betrachtet man aber einmal nur Art. 7 Abs. 4 EU-DS-GVO, beinhaltet dieser Absatz zwei wichtige Aussagen: Einerseits, dass dass eine solche Koppelung nicht grundsätzlich verboten ist, denn die Regelung schreibt nur die Berücksichtigung dieses Umstands vor, verbietet die Koppelung aber nicht. Andererseits, dass eine vorliegende Koppelung aber auch – abhängig vom Einzelfall – zur Unfreiwilligkeit und damit Unwirksamkeit führen kann.

Da viele der kostenfreien Angebote im Internet auf dem Tausch „Serviceerbringung gegen Daten(nutzung)" basieren und oft die Kostenfreiheit erst möglich machen, scheint die Regelung in Art. 7 Abs. 4 EU-DS-GVO in ihrer etwas weiteren Fassung als in dem Erwägungsgrund durchaus sinnvoll: Ein „Totalverbot" gibt es nicht, vielmehr muss im Einzelfall entschieden werden, wie freiwillig eine Einwilligung erteilt wird.

Bei Angeboten, die für das tägliche Leben wichtig sind, wie etwa die Eröffnung eines Bankkontos oder der Abschluss einer Versicherung, wird die Freiwilligkeit damit wohl deutlich strenger zu beurteilen sein, weil die Betroffenen auf solche Verträge angewiesen sind. Bei Verträgen dagegen, bei denen man die frei Wahl hat, wie etwa einem Buchversand im Internet, dürfte die Freiwilligkeit großzügiger bewertet werden.

Weitere Aussagen zur Freiwilligkeit enthalten die Erwägungsgründe 42 und 43, stellen u.a. darauf ab, wie groß das Ungleichgewicht zwischen dem Betroffene, der seine Einwilligung erteilen soll, und der verantwortlichen Stelle ist, vor allem sind Behörden genannt.

Neu: Zwingender Widerrufshinweis!

Eine weitere Neuerung ist, dass der Widerruf der Einwilligung so einfach möglich sein muss wie die Erteilung: Wenn man also in einer App per „Fingertipp" die Einwilligung erteilen kann, muss man in der App auch deren Widerruf per „Fingertipp" erklären können. Dies soll der „Beseitigung" einer unter Umständen vorschnell erteilten Einwilligung dienen, aber auch als Ausgleich, dass die strenge Schriftform nicht gefordert wird, dafür aber das „Loskommen" von einer Einwilligung erleichtert ist.

Ebenso neu ist die Vorgabe, dass schon bei Abfrage der Einwilligung und vor deren Erteilung der Betroffenen darüber zu informieren ist, dass er die Einwilligung später mit Wirkung für die Zukunft widerrufen kann (Art. 7 Abs. 3 EU-DS-GVO). In Deutschland ist aktuell dieser Hinweis im BDSG nicht vorgesehen, das TMG, das Internetsachverhalte regelt, kennt ihn dagegen. Ebenso gibt es eine ähnliche Pflicht im BDSG in Verbindung mit einer gesetzlichen Erlaubnis zur werblichen Nutzung und deren Widerspruch (demgemäß in § 28 Abs. 4 BDSG geregelt, nicht bei der Einwilligung in § 4 a BDSG oder § 28 Abs. 3 a BDSG).

Mit anderen Worten: Eine Einwilligung ist nach neuem Recht nur zulässig, wenn der Betroffenen vor Erteilung über das Widerrufsrecht hingewiesen wurde. Für neue Einwilligung lässt sich dies gut von Anfang an beachten, nicht aber für schon in der Vergangenheit erteile Einwilligungen. Dies kann betreffend des einleitend angesprochenen „Bestandsschutzes" erhebliche Auswirkungen haben, siehe im Folgenden.

Was ist zum 25.05.2018 mit „Alt-Einwilligungen"?

Die im Rahmen dieser Übersicht zuletzt noch zu erwähnende Regelung betrifft die Frage, was zum Stichtag am 25.05.2018 eigentlich mit Einwilligungen passiert, die zuvor erteilt wurden: Bleiben diese gültig? Immer oder nur in bestimmten Fällen? Wer entscheidet dies?

Die Frage ist von erheblicher Relevanz, wenn ein Unternehmen etwa viele Hunderttausend Einwilligungen über die Jahre hinweg gesammelt hat und die darauf basierende Datennutzung wesentlicher Teil des Geschäftsmodells ist.

Bemerkenswert ist, dass sich in den Artikeln der EU-DS-GVO zu dieser Frage nichts findet, sondern nur in einem Entscheidungsgrund, nämlich Nr. 171. Dort findet sich folgende Aussage: *„Beruhen die Verarbeitungen auf einer Einwilligung gemäß der Richtlinie 95/46/EG, so ist es nicht erforderlich, dass die betroffene Person erneut ihre Einwilligung dazu erteilt, wenn die Art der bereits erteilten Einwilligung den Bedingungen dieser Verordnung entspricht, so dass der Verantwortliche die Verarbeitung nach dem Zeitpunkt der Anwendung der vorliegenden Verordnung fortsetzen kann."*

Dies bedeutet, dass eine „Alt-Einwilligung" nur dann gültig bleibt, wenn

deren „Art“ mehr oder weniger zufällig dem neuen Recht entspricht. Im Umkehrschluss heißt dies aber, dass alle anderen „Alt-Einwilligungen“ unwirksam werden. Dies war in früheren Fassungen der Entwürfe der EU-DS-GVO noch anders, dort gab es teilweise einen echten Bestandsschutz. In der finalen und gültigen Fassung aber gilt nur noch vorstehend zitierte Regelung. Von einem „Bestandschutz“ kann man damit gerade nicht mehr sprechen, denn an bestehende Einwilligungen werden ab 25.05.2018 dieselben Anforderungen gestellt wie neu einzuholende Einwilligungen: Entweder erfüllen sie die neuen Anforderungen (und bleiben nur dann wirksam) oder nicht (und sind unwirksam).

Dies führt dazu, dass jedes Unternehmen (und Behörde), das eine Datenverarbeitung auf eine Einwilligung stützt, die nächsten beiden Jahre nutzen muss, um zu prüfen, ob Einwilligungen (bzw. deren „Art“, was auch immer damit genau gemeint ist – dies ist eine der vielen offenen Fragen) nach dem aktuellen Recht schon den neuen Anforderungen genügen: Denn nur solche Einwilligungen bleiben wirksam. Ansonsten sollten die zwei Jahre genutzt werden, Kunden mit Einwilligungen, die nicht der EU-DS-GVO entsprechen, schon jetzt auf neue Einwilligungen, die diese Anforderungen erfüllen, „umzustellen“.

Betrachtet man den Umstand, dass nach neuem Recht der Widerrufshinweis schon vor Erteilung der Einwillung erteilt werden muss und sieht dies als Anforderung auch für „Alt-Einwilligungen“, dürfe in vielen Fällen in Deutschland diese Anforderung bei „Alt-Einwilligungen“ nicht erfüllt sein: Denn nach aktuellem deutschen Recht bedarf es dieses Hinweises nicht zwingend. Solchermaßen eingeholte Einwilligungen wären dann zum 25.05.2018 unwirksam.

Insofern ist wichtig, etwaige Einwilligungen die nächsten beiden Jahre nicht nur am bis dahin gültigen aktuellen nationalen Recht auszurichten, sondern sogleich auch an den Vorgaben der EU-DS-GVO.

Fazit: Was ist also neu?

Damit liegen aus deutscher Sicht die Neuerungen der EU-DS-GVO zur Einwilligung vor allem in den Detailvorgaben, wie zum Beispiel der entfallenden Schriftform sowie Vorgaben rund um den Widerrufshinweis und der Art des Widerrufs. Damit sind zugleich aber sehr praxisrelevante Themen betroffen. Für den Betroffenen wird der Schutz trotz Wegfalls der echten Schriftform im Ergebnis wohl zumindest nicht schlechter und im Hinblick auf die digitale Welt jedenfalls zeitgemäßer. Ein „mehr“ an Schutz gibt es über die verstärkten Freiwilligkeits- und Widerrufsanforderungen.

Rechtsanwalt Dr. Robert Selk beschäftigt sich seit über 15 Jahren intensiv mit dem Datenschutz, ist im internationalen Konzernbereich als externer Datenschutzbeauftragter tätig und sowie Mitgründer und -gesellschafter einer Software- und Beratungsfirma im CRM- und Kundendatenbereich, ebenso wie u.a. Leiter des Fachausschusses „Datenschutz“ der Deutschen Gesellschaft für Recht und Informatik.

Werner Hülsmann

Die Europäische Datenschutzgrundverordnung und ihre Auswirkungen auf den betrieblichen Datenschutz

Mit der Europäischen Datenschutzgrundverordnung (DSGVO) gibt es auch im Bereich des betrieblichen Datenschutzes mehr oder weniger wesentliche Änderungen, die künftig zu beachten sind. Bei einigen Regelungen der DSGVO steht allerdings noch nicht fest wie sie zum Zeitpunkt des Gültigwerdens der DSGVO am 25. Mai 2018 aussehen werden. Die DSGVO enthält viele Konkretisierungsklauseln, einige davon muss der nationale Gesetzgeber bis zum Gültigwerden der DSGVO ausfüllen, andere kann er bis zu diesem Zeitpunkt oder auch später ausfüllen. Manche spezielle Regelungen, wie die zur Videoüberwachung öffentlich zugänglicher Räume, fallen weg, andere Regelungen werden konkretisiert und weitere neu eingeführt. Dieser Artikel gibt eine erste Übersicht zu den wichtigsten Auswirkungen der DSGVO auf den betrieblichen Datenschutz[1] in Deutschland.

Beschäftigtendatenschutz

In der DSGVO gibt es bedauerlicherweise keine speziellen Regelungen zum Beschäftigtendatenschutz. Vielmehr gibt Art. 88 der DSGVO den Mitgliedstaaten die Möglichkeit „durch Rechtsvorschriften oder durch Kollektivvereinbarungen“ spezielle Regelungen zum Beschäftigtendatenschutzgesetz zu erlassen. Die Bundesregierung plant – laut Aussagen eines Mitarbeiters der BfDI – den § 32 BDSG in das sogenannte „Ablösegesetz“[2] zu „retten“ und somit zumindest diese minimalistische Regelung zum Beschäftigtendatenschutz weiter gelten zu lassen.

Bereits bisher wurden „Kollektivvereinbarungen“, also Tarif- und Betriebsvereinbarungen, die Regelungen zum

Umgang mit Beschäftigtendaten enthalten, als „andere Rechtsvorschriften" im Sinne des § 4 Abs. 1 BDSG angesehen. Mit diesen Vereinbarungen konnte und wurde für deren Geltungsbereich der Beschäftigtendatenschutz für spezielle Bereiche geregelt. Durch die Regelung des Artikel 88 Abs. 1 bleibt diese Möglichkeit erhalten. Der Abs. 2 gibt einen Rahmen für derartige Vereinbarungen vor:

> *„Diese Vorschriften umfassen angemessene und besondere Maßnahmen zur Wahrung der menschlichen Würde, der berechtigten Interessen und der Grundrechte der betroffenen Person, insbesondere im Hinblick auf die Transparenz der Verarbeitung, die Übermittlung personenbezogener Daten innerhalb einer Unternehmensgruppe oder einer Gruppe von Unternehmen, die eine gemeinsame Wirtschaftstätigkeit ausüben, und die Überwachungssysteme am Arbeitsplatz."*

Daher sind die in den bereits bestehenden Betriebs- und Tarifvereinbarungen enthaltenen Regelungen dahingehend zu überprüfen, ob sie diesen Anforderungen genügen.

Die betrieblichen Datenschutzbeauftragten

Die DSGVO sieht bei Unternehmen anders als bei Behörden keine generelle Pflicht zur Bestellung eines Datenschutzbeauftragten vor. Ein betrieblicher Datenschutzbeauftragter ist dann zu benennen[3] wenn

- die Kerntätigkeit[4] des Verantwortlichen[5] oder des Auftragsverarbeiters in der Durchführung von Verarbeitungsvorgängen besteht, welche aufgrund ihrer Art, ihres Umfangs und/oder ihrer Zwecke eine umfangreiche regelmäßige und systematische Überwachung von betroffenen Personen erforderlich machen, oder wenn
- die Kerntätigkeit des Verantwortlichen oder des Auftragsverarbeiters in der umfangreichen Verarbeitung besonderer Kategorien von Daten gemäß Artikel 9 oder von personenbezogenen Daten über strafrechtliche Verurteilungen und Straftaten gemäß Artikel 10 besteht.[6]

Daneben eröffnet Art. 37 Abs. 4 Satz 1, erster Halbsatz DSGVO die Möglichkeit, dass „der Verantwortliche oder der Auftragsverarbeiter oder Verbände und andere Vereinigungen, die Kategorien von Verantwortlichen oder Auftragsverarbeitern vertreten, einen Datenschutzbeauftragten benennen". Sollte europäisches oder nationales Recht dies vorschreiben, dann müssen die genannten Stellen gemäß Art. 37 Abs. 4 Satz 1, zweiter Halbsatz DSGVO einen Datenschutzbeauftragten benennen. Diese Konkretisierungsklausel, die dem nationalen Gesetzgeber die Möglichkeit gibt, eigene weitgehende Regelungen zur Pflicht zur Benennung von Datenschutzbeauftragten beizubehalten oder zu erlassen, ist vor allem dem Europäischen Parlament und im Ministerrat der Deutschen Vertretung zu verdanken.

Deutsche Regelung zur Benennung betrieblicher Datenschutzbeauftragter

Laut Aussagen von Mitarbeitern der Bundesbeauftragten für den Datenschutz und die Informationsfreiheit (BfDI) sowie des Bundesministeriums für Justiz und Verbraucherschutz beabsichtigt die Regierung die bisherigen Regelungen für die Pflicht zur Bestellung betrieblicher Datenschutzbeauftragter unverändert in das „Ablösegesetz" zu übernehmen. Allerdings ist nicht sicher, ob es tatsächlich dazu kommt, da aus Kreisen der Wirtschaft manches Mal zu hören ist, dass die Institution der betrieblichen Datenschutzbeauftragten eine bürokratische Last sei. Diese Aussage war und ist zu Zeiten des BDSG falsch und wird auch zu Zeiten der DSGVO immer noch falsch sein: Unabhängig davon, ob in einem Unternehmen ein Datenschutzbeauftragter zu bestellen ist oder nicht, die Anforderungen des BDSG und künftig der DSGVO müssen kompetent umgesetzt werden. Hierbei ist ein Datenschutzbeauftragter, der die erforderlichen Fähigkeiten und Kenntnisse mitbringt, eine große Hilfe und Unterstützung für das Unternehmen.

Die Stellung und die Aufgaben der Datenschutzbeauftragten sind dagegen in der DSGVO geregelt und können von den nationalen Gesetzgebern nicht abgeändert werden.

Art. 37 Abs. 7 regelt nun unmissverständlich: „Der Verantwortliche oder der Auftragsverarbeiter veröffentlicht die Kontaktdaten des Datenschutzbeauftragten und teilt diese Daten der Aufsichtsbehörde mit." Damit ist sichergestellt, dass zum einen die Datenschutzaufsichtsbehörden und zum anderen die Betroffenen sich bei Bedarf auch direkt an die jeweiligen Datenschutzbeauftragten wenden können.

Stellung der betrieblichen Datenschutzbeauftragten[7]

An der Stellung der betrieblichen Datenschutzbeauftragten ändert sich grundsätzlich nichts. Sie müssen „frühzeitig in alle mit dem Schutz personenbezogener Daten zusammenhängenden Fragen eingebunden" werden. Die Datenschutzbeauftragten sind von den Verantwortlichen und den Auftragsverarbeitern bei der Erfüllung ihrer Aufgaben sowie beim Erhalt ihrer Fachkunde zu unterstützen. Die Datenschutzbeauftragten sind bezüglich der Ausübung ihrer Aufgaben weisungsfrei und dürfen wegen der Erfüllung ihrer Aufgaben nicht benachteiligt oder abberufen werden. Die Datenschutzbeauftragten berichten „unmittelbar der höchsten Managementebene". Einen ausdrücklichen Kündigungsschutz, wie nun schon seit einigen Jahren im § 4f Abs. 3 Satz 4 zu finden ist, kennt die DSGVO leider nicht. Dies lässt befürchten, dass Unternehmen wieder auf die Idee kommen, unbeliebte Datenschutzbeauftragte, die ihre Aufgaben ernst nehmen, betriebsbedingt – d.h. nicht wegen ihrer Aufgabenerfüllung – zu kündigen.

Während in § 4f Abs. 5 Satz 2 BDSG nur stand: „Betroffene können sich jederzeit an den Beauftragten für den Datenschutz wenden" regelt Art 38 Abs. 4 DSGVO nun „Betroffene Personen können den Datenschutzbeauftragten zu allen mit der Verarbeitung ihrer personenbezogenen Daten und mit der Wahrnehmung ihrer Rechte gemäß dieser Verordnung im Zusammenhang stehenden Fragen zu Rate ziehen". Diese Formulierung ist deutlich weiter gefasst, als die bisherige Regelung des BDSG. Wenn es Betroffene fordern, sind ihnen von den betrieblichen Datenschutzbeauftragten nicht nur Auskünfte zu den verarbeiteten personenbezogenen Daten

zu geben, sondern sie umfassend darüber zu beraten, welche Rechte sie im Zusammenhang mit diesen Verarbeitungen haben.

Nach wie vor sind die Datenschutzbeauftragten bei der Erfüllung ihrer Aufgaben an Geheimhaltung und Vertraulichkeit gebunden. Die bisherigen Regelungen zur Verschwiegenheitsverpflichtung für externe Datenschutzbeauftragte bei Berufsgeheimnisträgern wie ÄrztInnen oder RechtsanwältInnen können vom deutschen Gesetzgeber beibehalten werden.

Neu ist – zumindest die ausdrückliche genannte – Regelung, dass der Verantwortliche oder der Auftragsverarbeiter sicherstellen muss, dass andere Aufgaben und Pflichten, die der Datenschutzbeauftragte eventuell neben seiner Tätigkeit als Datenschutzbeauftragter für das Unternehmen erfüllen muss, „nicht zu einem Interessenkonflikt führen". Diese Forderung wurde zwar bisher von den Datenschutzaufsichtsbehörden und BDSG-Kommentatoren aus der von § 4f Abs. 2 Satz 1 BDSG geforderten Zuverlässigkeit des Datenschutzbeauftragten abgeleitet, war aber nicht direkt im BDSG enthalten.

Aufgaben der Datenschutzbeauftragten

Die Datenschutzbeauftragten „obliegen" gemäß Art. 39 Abs. 1 DSGVO „zumindest folgende Aufgaben:

- Unterrichtung und Beratung des Verantwortlichen oder des Auftragsverarbeiters und der Beschäftigten, die Verarbeitungen durchführen, hinsichtlich ihrer Pflichten nach dieser Verordnung sowie nach sonstigen Datenschutzvorschriften der Union bzw. der Mitgliedstaaten;
- Überwachung der Einhaltung dieser Verordnung, anderer Datenschutzvorschriften der Union bzw. der Mitgliedstaaten sowie der Strategien des Verantwortlichen oder des Auftragsverarbeiters für den Schutz personenbezogener Daten einschließlich der Zuweisung von Zuständigkeiten, der Sensibilisierung und Schulung der an den Verarbeitungsvorgängen beteiligten Mitarbeiter und der diesbezüglichen Überprüfungen;
- Beratung — auf Anfrage — im Zusammenhang mit der Datenschutz-Folgenabschätzung und Überwachung ihrer Durchführung gemäß Artikel 35;
- Zusammenarbeit mit der Aufsichtsbehörde und
- Tätigkeit als Anlaufstelle für die Aufsichtsbehörde in mit der Verarbeitung zusammenhängenden Fragen, einschließlich der vorherigen Konsultation gemäß Artikel 36, und gegebenenfalls Beratung zu allen sonstigen Fragen."

Während in § 4g Abs. 1 Satz 4 Ziff. 2 BDSG eine der Aufgaben der Datenschutzbeauftragten darin bestand „die bei der Verarbeitung personenbezogener Daten tätigen Personen durch geeignete Maßnahmen mit den Vorschriften dieses Gesetzes sowie anderen Vorschriften über den Datenschutz und mit den jeweiligen besonderen Erfordernissen des Datenschutzes vertraut zu machen" haben die Datenschutzbeauftragten die Verantwortlichen und die Auftragsverarbeiter sowie die Beschäftigten nach der DSGVO hinsichtlich ihrer Datenschutzverpflichtungen „zu unterrichten und zu beraten".

Deutlich höhere Geldbußen

Nach Art. 83 Abs. 1 DSGVO sollen die Aufsichtsbehörden bei Datenschutzverstößen Bußgelder verhängen, die „in jedem Einzelfall wirksam, verhältnismäßig und abschreckend" sind. Es wird künftig kaum mehr möglich sein, etwaige Bußgelder „aus der Portokasse" zu bezahlen. Die Höhe der Bußgelder kann bis zu 20 Millionen EUR oder bis zu 4% des weltweiten Umsatzes des Unternehmens betragen, je nachdem, welcher Betrag der höhere ist. Nach Art. 83 Abs. 3 werden mehrere Verstöße gegen die DSGVO, die „bei gleichen oder miteinander verbundenen Verarbeitungsvorgängen" erfolgen, gemeinsam mit der maximalen Geldbuße für den schwerwiegendsten geahndet. Aber dies wird deutlich höhere Geldbußen als bisher in Deutschland üblich waren auch nicht vermeiden. Die rechtzeitige und vorausschauende Umsetzung der datenschutzrechtlichen Anforderungen wird also schon bereits aus monetären Gründen ein wichtiges Ziel der Unternehmenspolitik werden.

Zu berücksichtigen ist auch, dass gegenüber den Bußgeldvorschriften des BDSG einige Bußgeldtatbestände hinzugekommen sind. So ist ein Verstoß gegen § 9 „Technische und organisatorische Maßnahmen" BDSG bisher nicht mit einem Bußgeld verwehrt, ein Verstoß gegen Art. 25 „Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen" DSGVO, in dem die Verpflichtung zur Umsetzung geeigneter technischer und organisatorischer Maßnahmen enthalten ist, ist mit einem Bußgeld bedroht.

Was ist neu?

Grundsätze der Datenverarbeitung

In Artikel 5 der DSGVO werden „Grundsätze für die Verarbeitung personenbezogener Daten" festgeschrieben. Diese sind:

1. „Rechtmäßigkeit, Verarbeitung nach Treu und Glauben, Transparenz",
2. „Zweckbindung",
3. „Datenminimierung",
4. „Richtigkeit",
5. „Speicherbegrenzung" (gemeint ist damit die frühestmögliche Anonymisierung der personenbezogenen Daten)[8], und
6. „Integrität und Vertraulichkeit"

Der Verantwortliche ist für die Einhaltung dieser Grundsätze verantwortlich und muss deren Einhaltung nachweisen können, in der DSGVO „Rechenschaftspflicht"[9] genannt. Zur Einhaltung der „Rechenschaftspflicht" wird es erforderlich, die im Unternehmen ergriffenen Maßnahmen zur Umsetzung des Datenschutzes und insbesondere der Grundsätze zumindest in elektronischer Form zu dokumentieren und diese Dokumentation aktuell fortzuschreiben.

Im Zusammenhang mit dem Grundsatz der „Speicherbegrenzung" ist zu beachten, dass gemäß Erwägungsgrund 26 DSGVO die einer „Pseudonymisierung unterzogene(n) personenbezogene(n) Daten, die durch Heranziehung zusätzlicher Informationen einer natürlichen Person zugeordnet werden könnten, (…) als Informationen über eine identifizierbare natürliche Person betrachtet werden (sollten)."

Pflicht, die Empfänger personenbezogener Daten über Löschung, Berichtigung und Sperrung zu informieren

Sofern es möglich und mit einem verhältnismäßigen Aufwand durchführbar ist, muss der Verantwortliche alle Empfänger der betreffenden personenbezogenen Daten über „jede Berichtigung oder Löschung der personenbezogenen Daten oder eine Einschränkung der Verarbeitung“[10] informieren. Darüber hinaus ist die betroffene Person auf Verlangen vom Verantwortlichen über die Empfänger der Daten zu informieren.

„Recht auf Datenübertragbarkeit“

Auch wenn auf den ersten Blick der Eindruck entstehen könnte, dass der Art. 20 DSGVO in erster Linie auf große Datensammler wie Facebook und Google abzielt, so gilt die Regelung, dass die betroffene Person „die sie betreffenden personenbezogenen Daten, die sie einem Verantwortlichen bereitgestellt hat, in einem strukturierten, gängigen und maschinenlesbaren Format zu erhalten“ hat um sie einem anderen Dienstleister zur Verfügung stellen zu können, für alle Daten, die Aufgrund einer Einwilligung oder auf Grund eines Vertragsverhältnisses automatisiert verarbeitet werden. Damit gilt diese Regelung z.B. auch für Online-Shop-Betreiber, Online-Spiele-Anbieter aber auch für die Beschäftigtendaten des Arbeitgebers.

Dokumentationspflichten

Wie oben dargestellt, fordert der Art. 5 der DSGVO, dass der Verantwortliche die Einhaltung der Grundsätze der Datenverarbeitung nachweisen kann. In Art. 24. wird von Verantwortlichen und Auftragsverarbeitern verlangt, dass sie „geeignete technische und organisatorische Maßnahmen (ergreifen), um sicherzustellen und den Nachweis dafür erbringen zu können, dass die Verarbeitung gemäß dieser Verordnung erfolgt.“. Für diese Nachweiserbringung ist es unerlässlich die umgesetzten technischen und organisatorischen Maßnahmen in ausreichender Detailliertheit zu dokumentieren und diese Dokumentation aktuell zu halten. Zu den Dokumentationspflichten gehört auch das „Verzeichnis von Verarbeitungstätigkeiten“ (aus dem BDSG als Verfahrensübersicht bekannt), das weiter unten dargestellt wird.

Was fällt weg?

Videoüberwachung

Spezielle Regelungen zur Videoüberwachung, wie sie in § 6b BDSG enthalten waren, sind in der DSGVO nicht enthalten. Sofern eine – auch nur kurzzeitige – Aufzeichnung der Videoüberwachung erfolgt, ist diese unstreitig als Verarbeitung personenbezogener Daten anzusehen, bei der die allgemeinen Regelungen der DSGVO[11] oder bei der Videoüberwachung von Beschäftigten auch die – wenn solche erlassen werden – speziellen Regelungen zum Beschäftigtendatenschutz gelten. Sofern nur eine Live-Beobachtung ohne Aufzeichnung erfolgt, ist noch zu klären, ob dies auch als Verarbeitung anzusehen ist. Wenn ja, würden auch hier die entsprechenden Datenschutzanforderungen gelten. Wenn nein, würden nur zivilrechtliche Regelugen, wie das allgemeine Persönlichkeitsrecht, greifen.

Mobile personenbezogene Speicher- und Verarbeitungsmedien

Gab es mit § 6c BDSG spezielle Regelungen für Mobile personenbezogene Speicher- und Verarbeitungsmedien[12], so sind mit Gültigwerden der DSGVO auf derartige Medien nur noch die Regelungen der DSGVO oder je nach Einsatzgebiet derartiger Medien die entsprechenden bereichsspezifischen Regelungen anzuwenden. Im betrieblichen Alltag kam § 6c BDSG allerdings selten zur Anwendung. Dessen Forderungen lassen sich zudem aus den in der DSGVO ausdrücklich aufgeführten Grundsätzen für die Verarbeitung personenbezogener Daten[13] und den Rechten der Betroffenen[14] ableiten.

Keine Verpflichtung mehr auf das Datengeheimnis

Begrifflich fällt das Datengeheimnis aus § 5 Abs. 1 BDSG[15] mit Gültigwerden der DSGVO weg. Art. 29 schreibt allerdings vor: „Der Auftragsverarbeiter und jede dem Verantwortlichen oder dem Auftragsverarbeiter unterstellte Person, die Zugang zu personenbezogenen Daten hat, dürfen diese Daten ausschließlich auf Weisung des Verantwortlichen verarbeiten“. Dies ist – ohne dass es so genannt würde – eine andere Formulierung des Datengeheimnisses.

Eine Regelung zur formalen Verpflichtung der Mitarbeiter eines Unternehmens auf das Datengeheimnis[16] kennt die DSGVO nicht. Ohne ein zusätzliches „Vertrautmachen“ mit den Datenschutzanforderungen am Arbeitsplatz hatte diese formale Verpflichtung allerdings auch bislang in der Regel keine Wirkung entfaltet. Art. 32 Abs. 4 DSGVO fordert: „Der Verantwortliche und der Auftragsverarbeiter unternehmen Schritte, um sicherzustellen, dass ihnen unterstellte natürliche Personen, die Zugang zu personenbezogenen Daten haben, diese nur auf Anweisung des Verantwortlichen verarbeiten“. Welche Schritte dies sind, lässt die DSGVO an dieser Stelle offen. Einer der Schritte wird aber sicherlich sein, die Beschäftigten auf die Regelung des Art. 29 DSGVO hinzuweisen. Einer formalen Verpflichtung auf diese Regelung bedarf es gemäß der DSGVO allerdings nicht.

Was bleibt?

Vieles, was aus dem BDSG bekannt und von daher in den Unternehmen bereits umgesetzt ist (oder worden sein sollte) findet sich – wenn auch mit gewissen Abweichungen – auch in der DSGVO. Ausgewählte Teilbereiche finden sich in den nachstehenden Abschnitten. Da die Darstellung aller dieser Regelungen den Rahmen dieses Artikels sprengen würde, findet sich in der anschließenden Übersicht eine Gegenüberstellung der entsprechenden Artikel der DSGVO zu den Paragraphen des BDSG.

Verzeichnis von Verarbeitungstätigkeiten

Das Führen der Verfahrensübersicht bzw. des „Verzeichnisses von Verarbeitungstätigkeiten“, wie es nun in der

DSGVO heißt, ist nun nicht mehr Aufgabe der Datenschutzbeauftragten, sondern ist eine Aufgabe, die die Unternehmen (Verantwortliche und Auftragsverarbeiter) gemäß Art. 30 DSGVO nun selbst verrichten müssen. In dieses Verzeichnis sind „Namen und die Kontaktdaten (…) eines etwaigen Datenschutzbeauftragten“ anzugeben. Bisher war diese Angabe in der Verfahrensübersicht freiwillig. Dieses Verzeichnis ist nun nicht mehr vom Datenschutzbeauftragten „jedermann in geeigneter Weise verfügbar“ zu machen sondern von dem Verantwortlichen oder Auftragsverarbeiter der Datenschutzaufsichtsbehörde auf Anfrage zur Verfügung zu stellen.

Im Übrigen entspricht der Inhalt des Verarbeitungsverzeichnisses im Wesentlichen den in § 4e BDSG enthaltenen Angaben. Während nach § 4e Ziffer 6 „Empfänger oder Kategorien von Empfängern, denen die Daten mitgeteilt werden können“ zu benennen waren, sind nach Art 30 Abs. 1 lit. d „die Kategorien von Empfängern, gegenüber denen die personenbezogenen Daten offengelegt worden sind oder noch offengelegt werden“ anzugeben. Bei Datenübermittlungen an Drittstaaten oder internationale Organisationen ist in bestimmten Fällen zu dokumentieren, dass es „geeignete Garantien“ für ein angemessenes Datenschutzniveau beim Empfänger gibt. Neu ist, dass in der DSGVO – im Gegensatz zum BDSG – ein Verstoß gegen die Regelungen zur Führung dieses Verzeichnisses mit einem Bußgeld bedroht wird.

Internationale Datenübermittlungen

Die bisherigen Möglichkeiten zum internationalen Datenaustausch, wie sie im betrieblichen Bereich gerade bei Unternehmen in international aufgestellten Unternehmensgruppen oder Konzernen erfolgt, bleiben auch mit der DSGVO grundsätzlich erhalten. In der DSGVO sind die entsprechenden Regelungen (Kapitel 5, Artt. 45-50 DSGVO) allerdings deutlich konkreter als die bisherigen Regelungen des BDSG.

Insbesondere bleibt die Möglichkeit erhalten, dass die Kommission durch einen Angemessenheitsbeschluss feststellt „dass das betreffende Drittland, ein Gebiet oder ein oder mehrere spezifische Sektoren in diesem Drittland oder die betreffende internationale Organisation ein angemessenes Schutzniveau bietet“[17] und damit der Datentransfer vorgenommen werden darf. Auch die bisherigen Instrumente „Standarddatenschutzklauseln“ und von der Aufsichtsbehörde zu genehmigende „verbindliche interne Datenschutzvorschriften“ bleiben erhalten. Unternehmen, die den Wegfall von Safe Harbor bereits berücksichtigt haben, werden durch das Gültigwerden der DSGVO keine unliebsamen Überraschungen für den internationalen Datenverkehr erleben.

Weitere Regelungen in der Übersicht

In der folgenden Übersicht sind die noch nicht dargestellten Regelungen aufgenommen, die bereits im BDSG enthalten waren und die grundsätzlich auch weiterhin in der DSGVO enthalten sind. Im Einzelnen können die bisherigen und die zukünftigen Regelungen inhaltlich allerdings mehr oder weniger deutlich voneinander abweichen. Daher ist auch bei den Regelungen in dieser Übersicht eine intensive Beschäftigung mit den neuen Formulierungen unvermeidlich.

Es gibt weiterhin – auch auf EU-Ebene – bereichsspezifische Regelungen, wie z.B. die EU-Datenschutzrichtlinie für die elektronische Kommunikation (Richtlinie 2002/58/EG), deren Regelungen durch die DSGVO nicht aufgehoben werden.

- Verbot mit Erlaubnisvorbehalt (Art. 6 DSGVO – § 4 BDSG)
- Regelungen zur Einwilligung[18] (Art. 7 DSGVO – §§ 4a, 28 Abs. 3a, 3b BDSG)
- Regelungen für die Verarbeitung besonderer Datenarten (Artt. 9 u. 10 DSGVO – § 28 Abs. 6 BDSG)
- Rechte der Betroffenen (Artt. 12-17 DSGVO – §§ 6, 7, 9 und 33-35 BDSG). Die Informationspflichten aus Artt. 13 und 14 DSGVO sind allerdings sehr viel umfangreicher als die Benachrichtigungsvorgaben des § 33 BDSG
- Regelungen zur automatisierten Einzelfallentscheidung (Art. 22 DSGVO – § 6a BDSG
- Die Pflicht, geeignete technische und organisatorische Maßnahmen zu treffen (Art. 24 Abs. 1 DSGVO – § 9 BDSG)
- Datenminimierung, datenschutzfreundliche Technik (Art. 25 Abs. 1 DSGVO – § 3a BDSG)
- Erforderlichkeitsprinzip (Art 25 Abs. 2 DSGVO – § 3a BDSG)
- Strikte Regelungen für die Auftragsdatenverarbeitung (Artt. 28 und 29 DSGVO – § 11 BSDG)
- Regelungen zu den technischen und organisatorischen Maßnahmen (Art. 32 DSGVO – Anhang zu § 9 BDSG)
- Meldepflicht von Datenschutzverletzungen an die Aufsichtsbehörde und Benachrichtigung der Betroffenen (Artt. 33 und 34 DSGVO – § 42a BDSG)
- Aus der Vorabkontrolle durch den Datenschutzbeauftragten wird die Datenschutz-Folgenabschätzung durch den Verantwortlichen (Art. 35 DSGVO – § 4d Abs. 5,6 BSDG)
- Meldepflicht bestimmter Verfahren (Art. 36 DSGVO – § 4e BDSG)
- Verhaltensregeln (Art. 40 DSGVO – § 38a BDSG)
- Freiwillige Zertifizierung (Art. 42 DSGVO – § 9a BDSG) Für die Datenschutzzertifizierung nach § 9a BDSG fehlte allerdings bislang das Umsetzungsgesetz, daher gab es freiwillige Zertifizierungen bisher nur auf landesrechtlicher Basis.

Fazit

Auch wenn viele der künftig geltenden Regelungen der DSGVO bereits derzeit schon im BDSG enthalten sind, sollten alle Unternehmen – unabhängig von ihrer Größe – die verbleibende Zeit bis zum 25. Mai 2018 nutzen, um die eigenen Datenverarbeitungen und die eigene Datenschutzorganisation – mit Unterstützung ihrer betrieblichen Datenschutzbeauftragten – an die Anforderungen der DSGVO und des noch zu verabschiedenden „Ablösegesetzes“ anzupassen.

1 Die DSGVO gilt zwar überwiegend gleichermaßen für öffentliche und nichtöffentliche Stellen (also für Behörden und private Unternehmen). Da aber derzeit für Behörden in Deutschland und in den Bundesländern andere Regelungen als für Unternehmen gelten, würde die Einbeziehung der Auswirkungen der DS-

GVO auf den behördlichen Datenschutz den Rahmen dieses Artikels sprengen.

2 „Ablösegesetz“ ist der Arbeitstitel für ein Gesetz, mit dem nach der derzeit bekannten Planung zum einen zum 25. Mai 2018 das bisherige BDSG vollständig aufgehoben werden soll und dass zum anderen sowohl die erforderliche Regelungen (z.B. im Bereich der Datenschutzaufsichtsbehörden) als auch weitere Regelungen zur Nutzung von einigen der Konkretisierungsklauseln enthalten soll.

3 Der Begriff der „Benennung eines/einer Datenschutzbeauftragten“ in der DSGVO ersetzt den Begriff der „Bestellung“ aus dem BDSG

4 Zum Begriff der „Kerntätigkeit“ sagt Erwägungsgrund 97 DSGVO: „Im privaten Sektor bezieht sich die Kerntätigkeit eines Verantwortlichen auf seine Haupttätigkeiten und nicht auf die Verarbeitung personenbezogener Daten als Nebentätigkeit.“

5 Der Begriff „Verantwortlicher“ aus der DSGVO ersetzt den Begriff „verantwortliche Stelle“ aus dem BDSG

6 Vgl. Art. 38 Abs. 1, lit b und c DSGVO

7 Vgl. Art. 38 Abs. 1 DSGVO

8 Vgl. Art. 5 Abs. 1 lit. e DSGVO: „Personenbezogene Daten müssen in einer Form gespeichert werden, die die Identifizierung der betroffenen Personen nur so lange ermöglicht, wie es für die Zwecke, für die sie verarbeitet werden, erforderlich ist“. Ausnahmen sind für im öffentlichen Interesse liegende Archivzwecke sowie für Wissenschaftliche und historische Forschungszwecke sowie für statistische Zwecke vorgesehen.

9 Vgl. Art. 5 Abs. 2 DSGVO

10 „Einschränkung der Verarbeitung“ ist grundsätzlich mit dem aus dem BDSG bekannten Begriff „Sperrung“ vergleichbar.

11 Vgl. hierzu: Thilo Weichert: „Die Europäische Datenschutz-Grundverordnung – ein Überblick“ in dieser Ausgabe

12 Das sind nach § 3 Abs. 10 BDSG „Datenträger, 1. die an den Betroffenen ausgegeben werden, 2. auf denen personenbezogene Daten über die Speicherung hinaus durch die ausgebende oder eine andere Stelle automatisiert verarbeitet werden können und 3. bei denen der Betroffene diese Verarbeitung nur durch den Gebrauch des Mediums beeinflussen kann“

13 Art. 5 DSGVO

14 Artt. 12-17 DSGVO

15 „Den bei der Datenverarbeitung beschäftigten Personen ist untersagt, personenbezogene Daten unbefugt zu erheben, zu verarbeiten oder zu nutzen (Datengeheimnis).“

16 Vgl. § 5 Satz 2 BDSG

17 Vgl. Art. 45, Abs. 1 DSGVO

18 Vgl. hierzu aber Erwägungsgrund (EWG) 32 der DSGVO sowie Artikel 8 „Bedingungen für die Einwilligung eines Kindes in Bezug auf Dienste der Informationsgesellschaft“ DSGVO

Auf den nächsten Seiten finden Sie Beiträge der folgenden Organisationen, Verbände und Einzelpersonen, die sich erneut mit den roten Linien, die sie in der DANA 3/2015 postuliert hatten, auseinandersetzen und in ihren Beiträgen Resümee ziehen, welche von den aufgestellten Forderungen in der EU-DSGVO eingehalten bzw. umgesetzt wurden. Manche Beiträge nutzen auch die Möglichkeit, den deutschen Gesetzgebern für die Gestaltung des BDSG-Ablösegesetzes Empfehlungen mitzugeben.

Die Beteiligten in alphabetischer Reihenfolge sind:
BfDI – Die Bundesbeauftragte für den Datenschutz und die Informationsfreiheit – www.bfdi.bund.de, BvD – Berufsverband der Datenschutzbeauftragten Deutschlands (BvD) e.V. – www.bvdnet.de, Digitalcourage – Digitalcourage e.V. – www.digitalcourage.de, Digitale Gesellschaft – Digitale Gesellschaft e. V. – www.digitalegesellschaft.de, GDD – Gesellschaft für Datenschutz und Datensicherheit (GDD) e.V. – www.gdd.de, Konferenz der Datenschutzbeauftragten des Bundes und der Länder (erneut vertreten durch die hessische Aufsichtsbehörde in Abstimmung mit der momentan den Vorsitz innehabenden Aufsichtsbehörde aus Mecklenburg-Vorpommern) – (u.a.) https://datenschutz-berlin.de/content/deutschland/konferenz, Prof. Douwe Korff – www.korff.co.uk/douwe, Peter Schaar – www.eaid-berlin.de, vzbv – Bundesverband der Verbraucherzentralen und Verbraucherverbände – Verbraucherzentrale Bundesverband e.V. (vzbv) – www.vzbv.de

Die Deutsche Vereinigung für Datenschutz e.V. dankt den beteiligten Organisationen, Verbänden und Einzelpersonen, die erneut Beiträge zur EU-DSGVO beigesteuert haben.











verbraucherzentrale
Bundesverband

BDfI – Andrea Voßhoff / Sven Hermerschmidt[1]

Rote Linien eingehalten? Zur Verabschiedung der Datenschutz-Grundverordnung

Mit der Verabschiedung der Datenschutz-Grundverordnung[2] stellt sich die Frage, ob sich ihr Text innerhalb der nach der Ratseinigung definierten roten Linien bewegt.[3]

I. Zur Datenschutz-Grundverordnung

Zentrale Frage war und ist, ob das bestehende Datenschutzniveau durch die Datenschutz-Grundverordnung beibehalten wird oder nicht. Der Gesamtbefund fällt hier überwiegend positiv aus. Die Verordnung bewegt sich sehr weitgehend in dem Rahmen, der durch die EU-Grundrechtecharta vorgegeben ist und stellt damit ein dem heutigen Standard vergleichbar hohes Datenschutzniveau sicher.

Mit der Aufrechterhaltung der wichtigsten Prinzipien, aber auch der Einführung neuer Elemente wie dem Marktortprinzip oder dem Recht auf Datenübertragbarkeit kann sich das Ergebnis durchaus sehen lassen.

Hinzukommt, dass die Kooperations- und Kohärenzmechanismen bei der aufsichtsbehördlichen Tätigkeit die europaweite Harmonisierung vorantreiben werden.

Kritik an den sehr allgemeinen und auslegungsbedürftigen Vorschriften der Datenschutz-Grundverordnung ist wohlfeil. Angesichts der Vielzahl völlig unterschiedlicher Interessen ist es ein Erfolg, dass sich 28 Mitgliedstaaten und das Europäische Parlament, das immerhin 4.000 Änderungsanträge zu behandeln hatte, auf einen gemeinsamen Text verständigt haben, dessen Regelungen es nun auszufüllen gilt. Auch wenn die Verordnung nicht alle Wünsche eines Datenschützers befriedigen kann, wird jetzt ganz entscheidend sein, dass die nationalen Gesetzgeber, die Rechtsanwender und die Aufsichtsbehörden die Regelungen im Sinne der Grundrechtecharta auslegen. Nicht zuletzt ist es besonders wichtig, dass die Betroffenen ihre Rechte wahrnehmen und die Zivilgesellschaft eine grundrechtsorientierte Anwendung des Datenschutzrechts immer wieder einfordert.

Vor einem Jahr habe ich mit der Zweckbindung und der Einwilligung zwei Themen herausgestellt, um damit beispielhaft den Verbesserungsbedarf für die Trilog-Verhandlungen aufzuzeigen. Deren Schicksal ist wiederum exemplarisch für die vorsichtig positive Bilanz der vierjährigen Verhandlungen.

1. Die Zweckbindung

Erfreulicherweise konnte sich das Europäische Parlament in den Trilog-Verhandlungen mit seiner strikt an den Grundrechten orientierten Position sehr weitgehend durchsetzen. Die Datenschutz-Grundverordnung verbleibt nun in ihrem Art. 5 Abs. 1 lit. b) bei dem Grundprinzip, dass personenbezogene Daten nur dann für andere Zwecke weiterverarbeitet werden dürfen, wenn der neue Zweck mit dem ursprünglichen Verarbeitungszweck vereinbar ist. Die Möglichkeiten, personenbezogene Daten auch zu nicht vereinbaren Zwecken weiterverarbeiten zu dürfen, sind stark eingeschränkt worden.

Gleichwohl sieht die Datenschutz-Grundverordnung einige nicht unbedeutende und zum Teil nicht unkritische Einschränkungen der Zweckbindung vor.

a) Die Weiterverarbeitung personenbezogener Daten zu im öffentlichen Interesse liegenden Archivzwecken, für wissenschaftliche oder historische Forschungszwecke oder für Statistikzwecke ist nach Art. 5 Abs. 1 lit. b) 2. Halbsatz DSGVO per se mit dem Ursprungszweck vereinbar. Damit wird für diese Zwecke eine sehr weitgehende Privilegierung vorgenommen, die gerade im Hinblick auf einen weiten Forschungsbegriff und der Unbestimmtheit des Begriffs „Statistik" nicht unkritisch ist. Hier werden die Aufsichtsbehörden in der praktischen Anwendung der Verordnung darauf achten müssen, dass diese Privilegierung nicht über deren eigentliche Intention hinaus ausgenutzt wird.

b) Art. 6 Abs. 4 DSGVO erlaubt in seinem Obersatz in zwei Fällen auch die Weiterverarbeitung zu solchen Zwecken, die nicht mit dem Ursprungszweck vereinbar sind. Einerseits ist dies auf der Basis einer Einwilligung möglich, was angesichts der Autonomie des Betroffenen konsequent ist.

Andererseits ist eine solche Zweckänderung möglich, wenn sie auf einer Rechtsvorschrift des Unions- oder mitgliedstaatlichen Rechts beruht. Diese Rechtsvorschrift muss eine „in einer demokratischen Gesellschaft (…) notwendige und verhältnismäßige Maßnahme zum Schutz der in Artikel 23 Absatz 1 genannten Ziele" darstellen. Dabei handelt es sich um wichtige öffentliche Interessen wie z. B. die Landesverteidigung, die nationale Sicherheit, aber auch fiskalische Interessen im Steuerbereich. Diese Möglichkeit der Zweckänderung muss die grundrechtliche Garantie der Zweckbindung im Blick haben und kann nur ausnahmsweise herangezogen werden. Insbesondere stellt Art. 6 Abs. 4 DSGVO keine Befugnis zum Erlass einer Rechtsvorschrift dar, sondern nimmt Bezug auf Rechtsvorschriften, die aufgrund der (anderen) Öffnungsklauseln der Datenschutz-Grundverordnung erlassen worden sind. Anderenfalls könnte Art. 6 Abs. 4 DSGVO – insbesondere in Verbindung mit Art. 23 Abs. 1 lit. i) DSGVO – als nahezu uferlose Öffnungsklausel für Regelungen vor allem im nicht-öffentlichen Bereich genutzt werden, was dem Harmonisierungsanspruch der Datenschutz-Grundverordnung zuwiderliefe.

c) Art. 6 Abs. 4 DSGVO stellt darüber hinaus Kriterien auf, die bei der Prüfung der Vereinbarkeit mit dem Ursprungszweck zu berücksichtigen seien. Hier ist vor allem Art. 6 Abs. 4 lit. e) DSGVO hervorzuheben, wonach auch Verschlüsselung oder Pseudonymisierung Instrumente sind, die zugunsten einer Zulässigkeit der Zweckänderung zu berücksichtigen sind. Gerade die Weiterverarbeitung pseudonymisierter Daten dürfte für Geschäftsmodelle, die auf der Nutzung von Big-Data-Anwendungen beruhen, von Bedeutung sein, da auf diese Weise Big-Data datenschutzkonform ausgestaltet werden kann.

2. Die Einwilligung

Anders als bei der Zweckbindung hat es bei den Anforderungen an die Einwilligung gegenüber der Ratsfassung vom 15. Juni 2015 keine wesentlichen Veränderungen mehr gegeben. Abgesehen von wichtigen Ausnahmen wird eine ausdrückliche Einwilligung unter der Datenschutz-Grundverordnung nicht notwendig sein. Nach der Definition in Art. 4 Abs. 11 DSGVO bedarf es lediglich einer „unmissverständlich abgegebenen Willensbekundung". Hier werden die Aufsichtsbehörden genau prüfen müssen, dass die Betroffenen ihr Einverständnis zurechenbar und in Kenntnis aller Umstände aktiv erteilen, damit die Grenzen zwischen opt-in und opt-out nicht zulasten der Betroffenen verwischt werden.

II. Zur Anpassung des nationalen Datenschutzrechts

Trotz des grundsätzlichen Anspruchs, mit der Datenschutz-Grundverordnung das Datenschutzrecht europaweit zu harmonisieren, enthält die Verordnung bekanntlich eine Vielzahl von Öffnungsklauseln, die die nationalen Gesetzgeber verpflichten oder es ihnen ermöglichen, mitgliedstaatliches Recht zu erlassen. Dies betrifft neben den institutionellen Fragen vor allem die Verarbeitung personenbezogener Daten im öffentlichen Bereich.

1. Eine starke Stimme für den deutschen Datenschutz in Europa

Angesichts der Kooperationsmechanismen, des Kohärenzverfahrens, aber auch des insgesamt gestiegenen Bedarfs an einer europaweit einheitlichen Anwendung des Datenschutzrechts wird die Zusammenarbeit der Aufsichtsbehörden in den 28 Mitgliedstaaten enorm an Bedeutung gewinnen.

Deutschland kann hier als föderaler Staat das Knowhow und die Erfahrung von insgesamt 18 staatlichen Aufsichtsbehörden in die Waagschale werfen, ein nicht zu unterschätzender Vorteil im Vergleich zu den insoweit fast ausschließlich zentral verfassten Mitgliedstaaten. Andererseits hat auch Deutschland als Mitgliedstaat letztlich nur eine Stimme im europäischen Konzert, wie Art. 68 Abs. 3 und 4 DSGVO zeigt. Demnach muss Deutschland einen gemeinsamen Vertreter für den Europäischen Datenschutzausschuss (EDSA) benennen. Darüber hinaus muss gem. Art. 51 Abs. 3 DSGVO sichergestellt werden, dass das Kohärenzverfahren auch in einem Staat mit föderaler Aufsicht funktioniert, weshalb nach EG 119 eine zentrale Anlaufstelle einzurichten ist.

Damit Deutschland dennoch mit einer starken und ernstzunehmenden Stimme spricht, bedarf es einer in der europäischen Zusammenarbeit mit ausreichenden Ressourcen versehenen Aufsichtsbehörde, die die genannten Aufgaben wahrnimmt. Der Bundesgesetzgeber sollte daher die BfDI zum gemeinsamen Vertreter bestimmen und die zentrale Anlaufstelle bei ihr einrichten. Zugleich müssen die Interessen und Kompetenzen der Aufsichtsbehörden der Länder im Rahmen ihrer nationalen Zuständigkeiten auch in Europa eine starke Rolle spielen. Deshalb ist es nicht zuletzt aufgrund der innerstaatlichen Kompetenzordnung des Grundgesetzes unabdingbar, dass sich immer auch ein Landesvertreter – in der Rolle als stellvertretendes Mitglied i. S. v. Art. 68 Abs. 3 DSGVO – unmittelbar im EDSA einbringen und damit das deutsche Gewicht in Europa erheblich verstärken kann. Nicht im numerischen, aber im faktischen Sinne.

2. Nutzung der nationalen Spielräume im Sinne des Datenschutzes

Angesichts der Vielzahl von nationalen Regelungsmöglichkeiten erwarte ich, dass die Gesetzgeber in Bund und Ländern diese Spielräume in einer Weise nutzen, die sich am Recht auf informationelle Selbstbestimmung orientiert.

Dazu gehört die weitergehende verpflichtende Bestellung betrieblicher Datenschutzbeauftragter ebenso wie die Schaffung eines Beschäftigtendatenschutzgesetzes. Darüber hinaus sind die Befugnisse der Aufsichtsbehörden, insbesondere eine Klagebefugnis sowie die für Deutschland bislang nicht vorhandenen Anordnungs- und Untersagungsbefugnisse im öffentlichen Bereich im Sinne einer wirksamen Datenschutzaufsicht auszugestalten.

Die Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder hat in einer Entschließung neben den genannten Themen weitere Punkte benannt, die Gesetzgeber berücksichtigen sollten.[4]

1 Die Autorin Voßhoff ist Bundesbeauftragte für den Datenschutz und die Informationsfreiheit, der Autor Hermerschmidt ist dort Referent und Leiter der Projektgruppe „Revision des Europäischen Datenschutzrechts".

2 Verordnung (EU) 2016/679, ABl. EU 2016, L 119/1

3 Voßhoff/Hermerschmidt, DANA 2015, 117

4 Entschließung „Stärkung des Datenschutzes in Europa – Nationale Spielräume nutzen" vom 6./7.4.2016, http://www.bfdi.bund.de/SharedDocs/

BvD – Thomas Spaeing

Roten Linien des BvD zur DS-GVO – so sieht’s aus!

Europa hat sich ein neues Datenschutzrecht gegeben, das ist eine gute Nachricht. Wirklich, in diesen Tagen muss man dies betonen: Die 28 Mitgliedsstaaten haben sich, nach über vier Jahren an Diskussionen und gewaltiger Anteilnahme von außen, auf ein, wenn auch nicht einheitliches, so doch in Grundsätzen gemeinsames Datenschutzrecht geeinigt. Eine gewaltige Leistung für 28 so verschiedene Staaten und dazu in diesen Tagen und bei den zahlreichen anderen großen Themen. Hierfür ist den zuständigen Akteuren zu danken!

Dass Datenschutz innerhalb Europas nun überall gleich funktioniert, darf man nicht erwarten. Die Öffnungsklauseln einerseits und die Unterschiedlichkeit in der Umsetzung andererseits bieten noch genügend Spielraum für deutlich auseinanderliegende Varianten und Anwendungen der neuen Regelungen. Doch dazu später mehr. Zunächst wollen wir einen Blick werfen auf die roten Linien des BvD vom Sommer 2015 – als noch gar nicht klar war, auf was EU-Parlament und EU-Rat sich am Ende einigen würden.

Der Grundrechtsschutz in der DS-GVO

Das Verbot mit Erlaubnisvorbehalt wird beibehalten (Art. 6 DS-GVO). Europa ist dem Ansatz der Prävention treu geblieben: Ohne Rechtsgrundlage keine Verarbeitung personenbezogener Daten. Obwohl zuletzt zur Ermöglichung neuer Geschäftsmodelle der Wegfall dieses Prinzips gefordert wurde – und teilweise immer noch gefordert wird, konnte hier der Schutz der natürlichen Person bei der Verarbeitung seiner Daten an Art. 8 der Charta der Grundrechte der EU ausgerichtet werden.

Das Verbotsprinzip ist also weiterhin die wichtigste Säule eines wirksamen Datenschutzes, der die Bewohner der EU davor bewahrt, den Einfluss und Überblick über die Verarbeitung ihrer Daten zu verlieren. Die Einhaltung dieses Prinzips wird weiterhin durch die Datenschutzaufsichtsbehörden in den Mitgliedsstaaten überwacht und – soweit noch vorhanden – auch durch die betrieblichen und behördlichen Datenschutzbeauftragten gewährleistet.

Zweckbindung bleibt

Auch bei der Zweckbindung sah es lange so aus, als ginge diese im Strudel der Interessen verloren. Durch die Regelung in Art. 5 Abs.1 lit. b DS-GVO wird die Zweckbindung im europäischen Datenschutzrecht verankert. Damit dürfen personenbezogene Daten wie bisher nur für eindeutige, festgelegte zulässige Zwecke verarbeitet werden. Zweckänderungen sind nur erlaubt, wenn die Änderungen mit dem ursprünglichen Erhebungszweck (Art. 5 Abs. 1 lit. b und Art. 6 Abs. 4 DS-GVO) vereinbar sind. Dabei werden jetzt auch Kriterien festgelegt, nach denen die Zulässigkeit einer Zweckänderung zu beurteilen ist. Zudem legt die DS-GVO der für die Verarbeitung verantwortlichen Stelle auch umfassende Informationspflichten auf (Artt. 13 und 14), so dass die Betroffenen weitaus umfassender als bisher über die Verarbeitungen zu informieren sind.

Insbesondere die Regelungen in Art. 6 Abs. 4 DS-GVO können aber unterschiedlich verstanden werden und hier bleibt abzuwarten, welche Lesart seitens der Aufsichtsbehörden und auch der Rechtsprechung vorgegeben werden. Eine Verschlüsselung stellt noch keine Garantie im Sinne dieser Regelung dar. Schon bisher wurde eine Verschlüsselung von Daten immer mal wieder auf eine Stufe mit anonymisierten oder pseudonymisierten Daten gestellt. Um dazu eine Aussage treffen zu können, ist aber stets zu prüfen, wie und mit welcher Güte verschlüsselt wird. Zudem ist ein Verschlüsselungsverfahren immer mit einem Haltbarkeitsdatum zu versehen, da allein durch den technischen Fortschritt ehemals sichere Verschlüsselungsmechanismen hinfällig werden. Bei diesen technischen Fragestellungen wird sich auswirken, dass die DS-GVO sich mehr auf Schutzziele ausrichtet, denn nur auf eine checklistenmäßige Abprüfung der Maßnahmen nach Anlage zu § 9 BDSG. Es wird dabei eine Ausrichtung nach dem „Stand der Technik“ erwartet, anstatt „anerkannte Regeln der Technik“, die mit einem niedrigeren Sicherheitsniveau ausgelegt werden.

Hier kommt auch den betrieblichen Datenschutzbeauftragten eine wichtige Rolle zu. Sie müssen die Zweckbindungen und Zweckänderungen sowie eine Maßnahmenergreifung nach Gesichtspunkten der Informationssicherheit prüfen und hierzu beraten, um Risiken für Betroffen wie auch Verarbeiter zu vermeiden.

Datenminimierung ersetzt Datensparsamkeit

An dieser Stelle muss eine zeitweilig ebenfalls durch Streichung bedrohte Regelung hingewiesen werden. Die Datensparsamkeit aus dem BDSG galt lange als umstritten und wurde nun mit der Regelung in Art. 5 Abs. 1 lit. c unter dem Begriff der Datenminimierung in die Grundsätze aufgenommen. Damit bleibt ein wesentliches Datenschutzprinzip auch auf europäischer Ebene gewahrt. Beide Regelungen sollen wahllose Big-Data-Analysen nach dem Prinzip „alles rein, dann schauen wir mal, was passiert“ verhindern und einen zielgerichteten Smart-Data-Ansatz fördern: Analysen nur mit den für den Zweck sinnvollen und zulässigen Daten durchzuführen.

Auch hier wird der Datenschutzbeauftragte wichtige Unterstützung leisten, indem er bereits bei der Konzeption von Analysen auf diese Prinzipien hinwirkt und hilft, kostenintensive Fehlanalysen zu vermeiden.

Wirksame Aufsichtsstrukturen

Für die Durchsetzung der Betroffenenrechte sind wirksame Aufsichtsstrukturen unerlässlich. Die DS-GVO hat hier mit den Regelungen in Artt. 51 ff die Voraussetzungen geschaffen, um die Aufsichtsbehörden EU-weit handlungsfähig zu machen. Es bleibt aber abzuwarten, ob und wie schnell die EU-Staaten diesen Vorgaben folgen werden. Zudem ist offen, ob die bisherige Praxis, Datenschutzrecht unterschiedlich zu interpretieren und daraus vollkommen andere Handlungen abzuleiten, durch die DS-GVO ein Ende hat. Auch in Deutschland wurde EU-Recht gelegentlich erst durch den EuGH zur Geltung verholfen. Bleibt die Umsetzungstreue der Mitgliedsstaaten derart schwach ausgeprägt, so wird die DS-GVO hier ein zahnloser Tiger. Aufsichtsbehörden ohne Kapazität und zudem noch an europäische Abstimmungsverfahren (Kohärenzverfahren) gebunden, werden keine Aufsicht ausüben und somit auch keine Sanktionen verhängen können.

Wir sehen, auch hier bieten sich den Mitgliedsstaaten Möglichkeiten, die DS-GVO ganz unterschiedlich umzusetzen. Der Zwang zur EU-weiten Abstimmung – so wichtig er für eine einheitliche Rechtspraxis ist – kann u. U. zudem zu einer regelrechten Lähmung des behördlichen Aufsichtssystems führen.

EU-weite Bestellpflicht des betrieblichen Datenschutzbeauftragten

Dies ist eine besondere Leistung: EU-weit müssen in bestimmten Fällen nun betriebliche und behördliche Datenschutzbeauftragte (bDSB) installiert werden. Während allerdings Behörden immer einen bDSB bestellen müssen, sind Unternehmen nur unter bestimmten Voraussetzungen dazu verpflichtet (s.a. CuA 4/2016, S. 8 ff, T. Weichert). Zu diesen Regelungen wurde zudem eine Öffnungsklausel in Art. 37 Abs. 4 DS-GVO dokumentiert, die nun durch die nationalen Gesetzgeber formuliert werden muss.

Um die DS-GVO für die deutsche Wirtschaft wirksam und wirtschaftlich umzusetzen, ist der betriebliche Datenschutzbeauftragte das bewährte Instrument. Damit die Unternehmen auch zukünftig durch ihren bDSB unterstützt werden, sollte der deutsche Gesetzgeber die Öffnungsklausel im Sinne der bewährten Regelungen nutzen und Klarheit schaffen. Der Interpretationsspielraum der DS-GVO kann so aufgelöst und die Erfahrung und das Know-how der bDSB weiterhin zielgerichtet eingesetzt werden. Hiervon profitieren Unternehmen und Betroffene gleichermaßen. Angesichts der erheblichen Ausweitung der Datenverarbeitungen in den nächsten Jahren hilft den Unternehmen die Vertrauensposition des Datenschutzbeauftragten das dringend benötigte Vertrauen der Kunden und Mitarbeiter in Unternehmen und dessen Datenverarbeitung zu erhalten und auszubauen.

In Zusammenhang mit dieser Öffnungsklausel sollte der deutsche Gesetzgeber – ganz im Sinne der bisherigen Regelungen – die in der DS-GVO fehlenden Regelungen zum bDSB weiterführen. Insbesondere ist die Verschwiegenheit des DSB in der DS-GVO nicht ausreichend geregelt. Hier sollten die bewährten Regelungen des BDSG übernommen werden. Ferner war der Kündigungsschutz im BDSG weitgehender als der Abberufungsschutz in der DS-GVO. Hier sollte in konsequenter Umsetzung der Unabhängigkeitsanforderungen an den bDSB ebenfalls auf die BDSG-Regelung zurückgegriffen werden.

Die DS-GVO hält somit zwei weitere Bestandteile der Aufsichtsstrukturen bereit:

- Der betriebliche Datenschutzbeauftragte wird auf EU-Ebene etabliert.
- Das Verbandsklagerecht wird gestärkt und damit eine weitere Aufsichtskompetenz vergeben.

Rechenschaftspflicht und Compliance

Die DS-GVO verschiebt das Gewicht im Datenschutz mehr in Richtung Compliance – die verarbeitenden Stellen müssen nachweisen, dass alles Notwendige zur Einhaltung der Regelungen unternommen wurde. Hier bieten sich nun verschiedene Möglichkeiten. Zunächst denkt man an umfassende Richtlinien und Dokumentationen zu allen Verarbeitungsschritten. Ein anderer Ansatz hat sich allerdings vielfach als pragmatisch und zielführend erwiesen: Ein Managementsystem. Wir kennen solche Lösungen beispielsweise aus den Bereichen Qualität, Informationssicherheit oder Umweltschutz.

Ein Datenschutzmanagementsystem ist der gebotene Ansatz, um die Anforderungen der DS-GVO wirtschaftlich und effizient in Unternehmen und Behörden umzusetzen. Darüber hinaus wird so die Grundlage für die in der DS-GVO geforderte Zertifizierung gelegt. Der Datenschutzbeauftragte steht im Zentrum des Datenschutzmanagementsystems. Auf Basis seiner Erfahrung und fachlichen Kompetenz ist er in der Lage, die Anforderungen der DS-GVO professionell in die Gestaltung eines Datenschutzmanagementsystems zu übertragen. Durch die zu einem solchen System gehörenden Prüfungen und Dokumentationen können die verarbeitenden Stellen ihrer Rechenschaftspflicht nachkommen und gegenüber den Aufsichtsbehörden transparent und nachvollziehbar die im Unternehmen etablierten Maßnahmen nachweisen.

Nicht wenige Unternehmen haben sich in den vergangenen Jahren bereits zu diesem Schritt entschlossen und profitieren so bereits heute von den bewährten Strukturen eines Datenschutzmanagementsystems, welches unschwer auf die neuen Anforderungen der DS-GVO angepasst werden kann.

Abschließend kann festgestellt werden, dass die DS-GVO, bei aller Vorsicht, auch viele Chancen bietet Verarbeitungen neu zu konzipieren und zu gestalten. Dadurch kann der Datenschutz in den Unternehmen und Behörden professionalisiert werden. Insofern sind die roten Linien des BvD zwar stellenweise strapaziert, aber unter Einbeziehung der Öffnungsklauseln doch eingehalten worden.

Ihr BvD-Ansprechpartner:
Vorstandsvorsitzender Thomas Spaeing, Budapester Straße 31, 10787 Berlin, Tel: 030 . 26 36 77 60,
E-Mail: bvd-gs@bvdnet.de,
Internet: https://www.bvdnet.de

digitalcourage – Friedemann Ebelt

Was taugt die neue Datenschutzgrundverordnung?

Ab 2018 werden persönliche Daten in der Europäischen Union durch die neue Datenschutzgrundverordnung geschützt. Jahrelang hat Digitalcourage den Weg dahin kritisch begleitet mit Aktionen und Advocacy. Welche unserer fünf roten Linien für starken Datenschutz wurden schließlich eingehalten?[1]

1. Prinzipien der Speicherung (50% erreicht)[2]

Datensparsamkeit: Wir haben gefordert, dass Artikel 5 (c) Datensammlungen auf das Notwendigste beschränkt. Die Verordnung legt nun fest: „personenbezogene Daten müssen (…) auf das für die Zwecke der Verarbeitung notwendige Maß beschränkt sein." Das Prinzip der Datensparsamkeit wurde damit abgeschwächt und den Zwecken der Verarbeitung untergeordnet. Das verlagert die Crux auf die Zweckbindung (siehe 2.).

Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen wird in Artikel 23 geregelt. Wir haben gefordert, dass Artikel 23 drei Kriterien enthält:

(1) Das Kriterium „state of the art technology" ist enthalten. Datenverarbeiter sollen beim Datensammeln den Stand der Technik berücksichtigen. Allerdings müssen hier gleichwertig die Kosten abgewogen werden. Das eröffnet erheblichen Spielraum.

(2) Das von uns geforderte Kriterium „international best practices" ist nicht in der Verordnung enthalten.

(3) Die Kriterien „technical and organisational measures" sind enthalten. Allerdings wird hier, entgegen unserer Forderung, das Beispiel Pseudonymisierung genannt.

Grundsätzlich ist es ein entscheidender Fortschritt, dass das Prinzip „data protection by design and by default" in der Verordnung verankert ist.

2. Zweckbindung ohne Ausnahmen (30% erreicht)

Eine strikte Zweckbindung schützt Bürger.innen vor ungewollter Profilbildung, vor übergriffigen Auswertungen, vor Datenhandel ohne Einverständnis und weiteren, unabsehbaren Eingriffen in ihre Grundrechte. Die darum von uns geforderte ersatzlose Streichung von Artikel 6 (4) wurde umgesetzt. Artikel 6 (3a) ist allerdings enthalten und erlaubt, unter einigen Bedingungen, unzweckmäßige Datenverarbeitung. Hier ist die Verarbeitung von persönlichen Daten möglich, vorbei an der Zustimmung der betroffenen Person und vorbei an den Gesetzen der Mitgliedstaaten.

3. Profilbildung nur mit expliziter Zustimmung (90% erreicht)

Artikel 20 reguliert automatisiertes individuelles Entscheiden und die Bildung von Profilen. Wir haben gefordert, dass Profilbildung nur erlaubt ist mit expliziter Zustimmung der betroffenen Personen. Denn die Auswertung und Verknüpfung von Bewegungs-, Kommunikations- oder Entscheidungsprofilen sind nicht abschätzbare Gefahren für die Privatsphäre. Artikel 20 der neuen Verordnung garantiert Betroffenen das Recht, dass keine Profile über sie angelegt werden. Dafür gibt es drei Ausnahmen: Betroffene willigen explizit in die Maßnahme ein, die Maßnahme ist für Vertragsangelegenheiten notwendig oder die Maßnahme ist durch das Gesetz des Mitgliedstaates rechtens.

Rat und Kommission wollten ursprünglich den Betroffenen lediglich ein Widerspruchsrecht einräumen. Die Arbeit für stärkeren Datenschutz hat sich an dieser Stelle ausgezahlt.

4 Auskunftsrechte immer kostenfrei! (60% erreicht)

Artikel 15 regelt, welche Daten Betroffene bei den Verarbeitern einsehen können. Das ist die Basis für das Recht auf informationelle Selbstbestimmung.

Wir haben gefordert, dass für Auskünfte keine Gebühren anfallen dürfen. Die neue Verordnung regelt, dass die erste (elektronische) Kopie der Daten kostenfrei zur Verfügung gestellt werden muss. Für jede weitere kann eine angemessene Gebühr erhoben werden.

Die Verordnung gibt Betroffenen umfangreiche Rechte auf Auskunft und Zugang. Das umfasst unter anderem: Zweck und Dauer der Verarbeitung, das Recht eine Beschwerde an die Aufsichtsbehörde zu richten und Informationen zur Logik und Nutzung von Profilen.

Wenn Daten an Dritte weitergegeben werden, haben Betroffene das Recht über die Sicherheit des Transfers nach Artikel 42 informiert zu werden.

5 Datenportabilität ermöglichen (100% erreicht)

Artikel 18 gibt Nutzer.innen das Recht, ihre Daten von einem Internet-Dienst zu einem anderen „mitzunehmen". Datenportabilität gibt die Möglichkeit, beispielsweise zwischen sozialen Netzwerken frei wählen zu können. Das ermöglicht Wettbewerb und verhindert Monopole. Digitalcourage hat gefordert, dass Nutzer.innen ihre Daten ohne Behinderung durch Verarbeiter bewegen können und dass ihnen dafür die Daten in üblichen elektronischen Formaten zur Verfügung gestellt werden müssen. Zudem haben Nutzer.innen mit der neuen Verordnung das Recht, die Daten direkt zwischen den Verarbeitern bewegen zu lassen.

Weiter mitgestalten!

Die Europäische Datenschutzgrundverordnung hat Rechte und Pflichten zwischen Staaten, Unternehmen und Nutzer.innen neu geordnet. Viele Übergriffe der Konzern-Lobby konnten verhindert werden. Trotz einiger Schwach-

stellen wurden entscheidende Regulierungen und Rechte erkämpft. Diese müssen jetzt genutzt werden. Das zu ermöglichen, ist die Aufgabe, die jetzt vor uns liegt. Eine weitere besteht darin, die noch offenen Spielräume datenschutzfreundlich zu gestalten.

1 Zum Zeitpunkt der Beitragserstellung existierte keine endgültige deutsche Übersetzung der Verordnung. Darum können hier verwendete Begriffe vom offiziellen Text abweichen.

2 Um übersichtlich zu sein, ist jeweils grob eingeschätzt, zu wie viel „Prozent“ unsere roten Linien eingehalten wurden.

Digitale Gesellschaft – Volker Tripp

Datenschutzgrundverordnung: Überfällige Reform mit Abstrichen

Ganze vier Jahre hat es seit dem Vorschlag der EU-Kommission bis zur Verabschiedung der Datenschutzgrundverordnung durch das Europäische Parlament gedauert. Insbesondere der Ministerrat, in dem die Regierungen der EU-Mitgliedsstaaten vertreten sind, verschleppte das Gesetzesvorhaben zur Vereinheitlichung des Datenschutzes in Europa immer wieder und versuchte, die Reform mit immer neuen Einwänden und Vorschlägen zu verwässern. Zentrale Datenschutzprinzipien wie die Zweckbindung, die Einwilligung der Betroffenen oder die Datensparsamkeit sollten insbesondere nach dem Willen der Vertreter Deutschlands, Großbritanniens und Frankreichs geschwächt und soweit wie möglich abgeschafft werden. Hintergrund des Bestrebens, diese Grundsätze aufzubohren, war die Hoffnung der Mitgliedsstaaten, auch in Europa Geschäftsmodelle auf der Grundlage von „Big Data“, also dem Auswerten riesiger Datenmengen, zu befördern.

Glücklicherweise konnte sich der Ministerrat mit seiner überaus wirtschafts-, aber wenig datenschutzfreundlichen Haltung im Ergebnis nur bedingt durchsetzen. Obwohl das Europäische Parlament zumeist Schlimmeres verhindern konnte, hätte die Verordnung an vielen Stellen gleichwohl präziser, expliziter und konsequenter ausfallen können.

So hätte etwa bei der Einwilligung der Nutzerinnen und Nutzer in die Verarbeitung ihrer Daten durchaus mehr erreicht werden können. Nur bei besonders sensiblen Daten verlangt die Verordnung eine ausdrückliche Einwilligung. In allen anderen Fällen lässt sie eine zweifelsfreie Einwilligung, etwa durch konkludentes Handeln, ausreichen. Dadurch entstehen neue Grauzonen, welche die Datensouveränität der Nutzerinnen und Nutzer eher schwächen als stärken. Schließlich ist die Einwilligung die wichtigste Voraussetzung für die Zulässigkeit der Verarbeitung personenbezogener Daten.

Obendrein hat sich der Gesetzgeber an zahlreichen Stellen der Verordnung auch vor einem echten Ausgleich zwischen den Interessen der Betroffenen einerseits und denen der datenverarbeitenden Unternehmen andererseits gedrückt. Häufig werden schwammige und auslegungsbedürftige Begriffe verwendet, so dass unklar bleibt, wie der Ausgleich in der Praxis genau ausfallen wird. Unternehmen haben beispielsweise das Recht, personenbezogene Daten auch ohne Einwilligung der Betroffenen zu verarbeiten, wenn sie ein „berechtigtes Interesse“ an der Verarbeitung haben. Da die Verordnung diesen Begriff selbst nicht näher definiert, werden letztlich Aufsichtsbehörden und Gerichte entscheiden müssen, wann ein solches Interesse vorliegt.

Anhand der Häufigkeit, mit der solche unbestimmten Rechtsbegriffe in der Datenschutzgrundverordnung Verwendung finden, lässt sich auch gut ablesen, wie schwierig es für die Gesetzgebungsorgane der EU war, sich auf einen Text zu einigen. An insgesamt mehr als 60 Stellen der Verordnung finden sich nationale Öffnungsklauseln, die teils elementare Regelungen betreffen. Dies schwächt die Harmonisierungswirkung der Verordnung ganz erheblich und rückt das Ziel, Europa in eine echte Datenunion mit einheitlichen Schutzstandards zu verwandeln, in weite Ferne.

In einigen Punkten konnten jedoch auch Fortschritte erzielt werden. Besonders erfreulich ist etwa, dass das Prinzip der Datensparsamkeit nunmehr nicht nur europaweit gesetzlich verankert wurde, sondern sogar bereits in der Gestaltungsphase neuer Systeme und Algorithmen zu berücksichtigen ist. Das mag zwar insbesondere von Anbietern, die mit „Big Data“-Geschäftsmodellen liebäugeln, als Belastung und als Einschränkung ihrer unternehmerischen Freiheit empfunden werden. Die Stärkung der Datensparsamkeit könnte allerdings auch einen Innovationsschub bei den Geschäftsmodellen datenverarbeitender Unternehmen auslösen und so langfristig dazu beitragen, Europa als „Kontinent des Datenschutzes“ zu etablieren.

Auch ein weiteres Kernprinzip des Datenschutzes, die Zweckbindung, konnte glücklicherweise erhalten und in der Verordnung festgeschrieben werden. Gerade im Zusammenspiel mit den ebenfalls vorgesehenen Informationspflichten leistet die Zweckbindung einen wichtigen Beitrag zur Stärkung der Datensouveränität. Vor jeder Erhebung, Verarbeitung oder Nutzung ihrer personenbezogenen Daten müssen die Betroffenen über sämtliche entscheidungsrelevanten Umstände sowie den Zweck in leicht verständlicher Form in Kenntnis gesetzt werden. Im Verhältnis zur bisherigen Rechtslage in Deutsch-

land ist das zwar keine echte Neuerung; da jedoch auch das Marktortprinzip in der Verordnung verankert wurde, müssen sich nun sämtliche datenverarbeitenden Unternehmen, die in der EU Geschäfte machen, an diese Regeln halten. Die Aufsichtsbehörden, bisher oft als zahnlose Tiger verspottet, können Verstöße zudem mit Bußgeldern von bis zu 4 % des weltweiten Jahresumsatzes ahnden.

Bundesregierung und Bundestag stehen nun vor der großen Aufgabe, die deutsche Rechtslage an die Vorgaben der Verordnung anzupassen. Dies bedeutet einerseits, dass zahlreiche bestehende Gesetze wie das Bundesdatenschutzgesetz oder das Telemediengesetz zu großen Teilen aufgehoben werden müssen, um redundante oder abweichende nationale Regelungen zu vermeiden. Andererseits müssen die zahlreichen Öffnungsklauseln in deutsches Recht umgesetzt werden. Dabei wird sich zeigen, ob Bundesregierung und Bundestag den Geist der Reform verinnerlicht haben oder eher versuchen werden, ihn weiter zu verwässern. Mit der Verabschiedung der Datenschutzgrundverordnung haben die Befürworter des Datenschutzes eine wichtige Schlacht gewonnen, den Krieg hingegen noch lange nicht.

GDD – Andreas Jaspers

Der Datenschutzbeauftragte in der Datenschutz-Grundverordnung – Handlungsbedarf des deutschen Gesetzgebers

Bestellpflicht mit Öffnungsklausel

Eine der Innovationen des neuen europäischen Datenschutzrechts stellt die verpflichtende Bestellung von behördlichen und betrieblichen Datenschutzbeauftragten auf europäischer Ebene dar. Während die EU-Datenschutzrichtlinie von 1995 die Bestellung nur fakultativ vorsah, ist diese europaweit für Behörden oder öffentliche Stellen verpflichtend. Für die Privatwirtschaft ist die Bestellung aber nur bei Unternehmen obligatorisch, deren „Kerntätigkeit aus Verarbeitungsvorgängen besteht, welche auf Grund ihres Wesens, ihres Umfangs und/oder ihrer Zwecke eine regelmäßige und systematische Beobachtung von betroffenen Personen erforderlich machen“. Ebenso sollen nur Datenverarbeiter, deren Kerntätigkeit aus der Verarbeitung besonderer Kategorien von Daten gemäß Artikel 9 und 10 der DS-GVO „in großem Umfang“ besteht, einer Bestellpflicht unterfallen.

Die Pflicht zur Bestellung eines Datenschutzbeauftragten soll sich künftig nicht nur aus der DS-GVO selbst ergeben können. Insbesondere aufgrund des Bestrebens Deutschlands im Rahmen der Verhandlungen zur DS-GVO wurde in Art. 37 Abs. 4 DS-GVO eine Öffnungsklausel vorgesehen, die es ermöglicht, auf der Ebene des EU-Rechts bzw. des nationalen Rechts im Verhältnis zur DS-GVO weitergehende Verpflichtungen zur Bestellung von Datenschutzbeauftragten vorzusehen. Art. 37 Abs. 4 DS-GVO stellt überdies klar, dass die freiwillige Bestellung von Datenschutzbeauftragten unbenommen ist.

Der deutsche Gesetzgeber sollte die Öffnungsklausel nutzen und die bewährten Bestellvoraussetzungen, wie sie aktuell in § 4f Abs. 1 BDSG geregelt sind, beibehalten. Da die Voraussetzungen nach der DS-GVO für eine Bestellpflicht nur von einer sehr kleinen Anzahl von Unternehmen erfüllt werden, wäre sonst die Konsequenz, dass in Deutschland die Bestellung betrieblicher Datenschutzbeauftragter in Industrie, Handel und Mittelstand mit Geltung der DS-GVO auslaufen würde. Betroffene hätten einen Anwalt für ihre Rechte und Interessen in den Unternehmen verloren. Zugleich wäre für die Unternehmensleitung der unabhängige Berater und Garant der Selbstkontrolle auf betrieblicher Ebene wegfallen.

Von daher ist die von der GDD geforderte und vom Bundesinnenministerium für zwingend erklärte zusätzliche nationale Öffnungsklausel in Art. 37 Abs. 4 DS-GVO für die betriebliche Selbstkontrolle von großer Bedeutung. Damit kann in Deutschland die Selbstkontrolle auf betrieblicher Ebene durch einen unabhängigen Berater erhalten bleiben. Das Bundesinnenministerium hat angekündigt, die Bestellungsvoraussetzungen für einen betrieblichen Datenschutzbeauftragten in einem Verordnungsergänzungsgesetz gegenüber dem BDSG unverändert zu regeln. Es käme damit auch einem Beschluss des Deutschen Bundestages nach, wonach die Bundesregierung aufgefordert wird, „das in Deutschland bestehende und bewährte System der Beauftragten für den Datenschutz in Unternehmen und der Verwaltung“ in der EU-DS-GVO nicht zu gefährden (BT-Drs. 17/11325, Abschnitt II., Nr. 21).

Abberufungsschutz, aber kein Kündigungsschutz

Der Datenschutzbeauftragte darf nach der Grundverordnung nicht wegen der Erfüllung seiner Aufgaben benachteiligt oder abberufen werden (Art. 38 Abs. 3). Der Abberufungsschutz ist jedoch nicht durch einen arbeitsrechtlichen besonderen Kündigungsschutz wie in § 4f Abs. 3 Satz 5 und 6 BDSG flankiert. Dieser ist mit der Novelle aus dem Jahr 2009 in das BDSG aufgenommen worden, da der Abberufungsschutz eines betrieblichen (Teilzeit-)Datenschutzbeauftragten nach

der Rechtsprechung bis dahin nie zu einem Kündigungsschutz geführt hatte. Hier ist wieder der deutsche Gesetzgeber gefragt, den Datenschutzbeauftragten auch arbeitsrechtlich abzusichern.

Verschwiegenheitspflicht

Ein weiterer Handlungsbedarf besteht bei der Verschwiegenheitspflicht des Datenschutzbeauftragten. Nach Art. 38 Abs. 4 DS-GVO können betroffene Personen den Datenschutzbeauftragten zu allen mit der Verarbeitung ihrer personenbezogenen Daten und mit der Wahrnehmung ihrer Rechte aus der Verordnung in Zusammenhang stehenden Fragen zu Rate ziehen. Diese Regelung entspricht im Wesentlichen der nationalen Regelung in § 4f Abs. 5 Satz 2 BDSG, wonach sich Betroffene jederzeit an den Beauftragten für den Datenschutz wenden können. Nach bestehendem Recht steht die Tätigkeit des Datenschutzbeauftragten als „Anwalt der Betroffenen“ in engem Zusammenhang zu dessen Verschwiegenheitspflicht aus § 4f Abs. 4 BDSG. Nach dieser Regelung ist der Datenschutzbeauftragte zur Verschwiegenheit über die Identität des Betroffenen sowie über Umstände, die Rückschlüsse auf diesen zulassen, verpflichtet, soweit er nicht hiervon befreit wird. Besondere Bedeutung erlangt die Verpflichtung zur Wahrung der Vertraulichkeit im Bereich des Beschäftigtendatenschutzes, drohen doch ggf. karrieremäßige Nachteile, wenn bekannt wird, dass sich ein Mitarbeiter zwecks Überprüfung der Verarbeitung seiner personenbezogener Daten an den Datenschutzbeauftragten gewandt hat. Eine vergleichbare Pflicht wie in § 4f Abs. 4 BDSG ist in der DS-GVO nicht vorgesehen. Festgestellt wird nur, dass der Datenschutzbeauftragte nach dem Recht der Union oder der Mitgliedstaaten bei der Erfüllung seiner Aufgaben an die Wahrung der Geheimhaltung oder der Vertraulichkeit gebunden ist (Art. 38 Abs. 5 DS-GVO). Insofern ist es dringend geboten, die bisherigen nationalen Vorschriften zur Verschwiegenheit des Datenschutzbeauftragten aufrechtzuerhalten. Hierzu zählen auch § 4f Abs. 4a BDSG und § 203 Abs. 2a StGB.

Verstärkte Compliance-Funktion

Die Aufgaben der betrieblichen und behördlichen Datenschutzbeauftragten sind durch eine verstärkte Compliance-Funktion gekennzeichnet. Operative Aufgaben des BDSG wie die Schulung der Mitarbeiter oder die Programmprüfung entfallen. Die Datenschutzfolgenabschätzung, die die Vorabkontrolle ablöst, fällt in die Verantwortung des Unternehmens oder der Behörde. Der Datenschutzbeauftragte ist aber gemäß Art. 35 Abs. 2 DS-GVO in die Datenschutzfolgeabschätzung einzubinden. Damit entfällt auch die „Zweifelsfallregelung“, die dem Datenschutzbeauftragten die Pflicht auferlegt, selbständig die Aufsichtsbehörde zu konsultieren. Gleichwohl ist er gemäß Art. 39 Abs. 1 lit. e DS-GVO Ansprechpartner für die Aufsichtsbehörden in allen Datenschutzfragen inklusive im Verfahren der vorherigen Konsultation nach Art. 36 DS-GVO.

Die Rechtstellung des Datenschutzbeauftragten gemäß Art. 38 DS-GVO ist vergleichbar mit der gemäß BDSG. So agiert er weisungsfrei, bei gleichzeitiger unmittelbarer Berichtsmöglichkeit gegenüber der höchsten Managementebene. In diesem Zusammenhang erfolgt auch die Klarstellung, dass eine Unternehmensgruppe einen einzelnen Beauftragten für den Datenschutz bestellen kann (Art. 35 Abs. 2 DS-GVO)

Der Entwurf der DS-GVO beinhaltet keine abschließende Aufgabenzuweisung. Dies unterstreicht Art. 38 Abs. 6 DS-GVO, der die Wahrnehmung anderer Aufgaben nur unter den Vorbehalt eines Interessenkonflikts stellt. Sollen vom Datenschutzbeauftragten über den normativ verbindlich geregelten Bereich hinaus Aufgaben übernommen werden, bedarf es einer entsprechenden Zuweisung in der Stellenbeschreibung. Hier sind Arbeitgeber und Datenschutzbeauftragter gefragt.

Konferenz der Datenschutzbeauftragten des Bundes und der Länder – Prof. Dr. Michael Ronellenfitsch, Barbara Dembowski, Michael Kaiser, Maria Christina Rost, Julia Stoll, Dr. Rita Wellbrock

Stärkung des Datenschutzes in Europa – nationale Spielräume

Am 4. Mai 2016 wurde die Datenschutz-Grundverordnung (DSGVO, Verordnung (EU) 2016/679) im Amtsblatt der EU veröffentlicht. Bis zum 25. Mai 2018 haben die nationalen Gesetzgeber nun Zeit, die nationalen Spielräume zu analysieren und auszugestalten.

1. Sozial- und Gesundheitsbereich

Für die Verarbeitung von Sozial- und Gesundheitsdaten sind die Art. 6 (Rechtmäßigkeit der Verarbeitung) und Art. 9 der DSGVO (besondere Kategorien personenbezogener Daten) von zentraler Bedeutung.

Gemäß Art. 6 Abs. 2 können die Mitgliedstaaten spezifischere Bestimmungen zur Anpassung der Anwendung der Vorschriften der DSGVO in Bezug auf die Verarbeitung zur Erfüllung von Abs. 1 lit. c) und lit. e) beinhalten oder einführen, indem sie spezifische Anforderungen für die Verarbeitung sowie

sonstige Maßnahmen präziser bestimmen, um eine rechtmäßig und nach Treu und Glauben erfolgende Verarbeitung zu gewährleisten. Gemäß Art. 6 Abs. 1 lit. e) ist die Verarbeitung personenbezogener Daten rechtmäßig, wenn die Verarbeitung für die Wahrnehmung einer Aufgabe erforderlich ist, die im öffentlichen Interesse liegt oder in Ausübung hoheitlicher Gewalt erfolgt, die dem für die Verarbeitung Verantwortlichen übertragen wurde. Diese Voraussetzungen werden im Hinblick auf zahlreiche gesetzliche Regelungen im Sozial- und Gesundheitsbereich bejaht werden können, z.B. im SGB. Die Öffnungsklausel des Art. 6 Abs. 2 erlaubt dem nationalen Gesetzgeber Konkretisierungen und Präzisierungen, jedoch keine grundsätzlichen Änderungen der DS-GVO. Soweit Gesundheitsdaten (Art. 4 Abs. 15) verarbeitet werden, ist besonders Art. 9 zu beachten. Art. 9 Abs. 1 enthält ein Verarbeitungsverbot für besondere Kategorien personenbezogener Daten, d.h. Daten, die als besonders schützenswert bewertet werden. Gemäß Art. 9 Abs. 2 gibt es Ausnahmen von diesem Verarbeitungsverbot. Als weitere Einschränkung der Ausnahmen vom Verarbeitungsverbot sieht Art. 9 Abs. 3 vor, dass eine Datenverarbeitung zu den in Art. 9 Abs. 2 genannten Zwecken nur dann zulässig ist, wenn die datenverarbeitenden Personen besonderen, auf nationalem oder europäischem Recht basierenden, Geheimhaltungspflichten unterliegen.

Die Voraussetzungen des Art. 9 Abs. 2 werden im Hinblick auf zahlreiche gesetzliche Regelungen im Gesundheitsbereich bejaht werden können, z.B. im Hinblick auf das Infektionsschutzgesetz. Die Vorgaben des Art. 9 Abs. 3 werden durch die in Deutschland vorhandenen Regelungen zur ärztlichen Schweigepflicht und zum Sozialgeheimnis erfüllt.

Schließlich erlaubt Art. 9 Abs. 4 den Mitgliedstaaten, weitere Bestimmungen, einschließlich Beschränkungen zur Verarbeitung genetischer Daten, biometrischer Daten oder Gesundheitsdaten, beizubehalten oder einzuführen. Der nationale Gesetzgeber darf daher im Hinblick auf die Verarbeitung besonderer Kategorien personenbezogener Daten nicht nur Konkretisierungen vornehmen, sondern auch die sich aus der DSGVO ergebenden Verarbeitungsbefugnisse beschränken. Im Erwägungsgrund 53 wird darauf hingewiesen, dass die nationalen Regelungen jedoch den freien Verkehr personenbezogener Daten innerhalb der Union nicht beeinträchtigen sollte. Ob und wie der Gesetzgeber davon Gebrauch macht, kann zum jetzigen Zeitpunkt nicht abschließend bewertet werden.

2. Auskunfteienwesen

Die spezifischen Sondervorschriften für Auskunfteien, die bisher in den §§ 28a ff. BDSG enthalten und von einem breiten Konsens zwischen den Aufsichtsbehörden und den Auskunfteien getragen sind, fallen durch die DSGVO vollständig weg. Dadurch ist die Rechtssicherheit gefährdet und es droht eine erhebliche Ausweitung der von Auskunfteien gespeicherten, übermittelten und für Scoringzwecke genutzten Daten.

Die von Auskunfteien genutzten Daten sind wegen ihrer Entscheidungserheblichkeit im privaten Rechtsverkehr in ganz besonderem Maße dazu geeignet, die Rechte von Betroffenen zu beeinträchtigen.

Durch den Erhalt der Inhalte von § 28a BDSG in einem nationalen Gesetz sollten daher die Besonderheiten der deutschen Auskunfteienlandschaft berücksichtigt und die Rechte der Betroffenen gestärkt werden.

3. Auskunftspflichten

Aus § 34 Abs. 2 Satz 1 Nr. 1 und § 34 Abs. 4 BDSG ergeben sich umfangreiche Auskunftspflichten, die auf Scorewerte im Sinne des § 28b BDSG gerichtet sind. Macht eine betroffene Person ihre Auskunftsrechte geltend, kann sie die Auswirkungen des Scorings durch Erhalt von kürzlich übermittelten und aktuellen Scorewerten besonders gut einschätzen. Letztlich sind die Scorewerte das Datum mit der höchsten Entscheidungsrelevanz. Zwar enthalten die Artt. 13 Abs. 2 lit. f), 14 Abs. 2 lit. g) und 15 Abs. 1 lit. h) DSGVO auf die automatisierte Entscheidungsfindung und das Profiling gerichtete Auskunftspflichten, die auch die Tragweite und die angestrebten Auswirkungen dieser Verarbeitung auf den Betroffenen umfassen. Diese sind jedoch nicht auf die kürzlich übermittelten und aktuellen Score-, bzw. Profilingwerte konkretisiert. Stattdessen ergibt sich aus Erwägungsgrund 64 DS-GVO, dass Daten nicht alleine zu dem Zweck der Auskunftserteilung gespeichert werden sollen. Werden die übermittelten Score-, bzw. Profilingwerte daher nicht gespeichert, ist zu befürchten, dass diese der betroffenen Person nicht mehr mitgeteilt werden.

Zur Konkretisierung der Auskunftspflichten sollte daher in einem nationalen Gesetz klargestellt werden, dass die Übermittlung der Score- bzw. Profilingwerte zur Darlegung der Auswirkungen des Profilings auf die betroffene Person erforderlich ist.

4. Datenschutz-Folgenabschätzung

Mit der Durchführung einer Datenschutz-Folgenabschätzung (Art. 35) bei ggf. auch vorheriger Konsultation (Art. 36) soll ein hohes Risiko für die Rechte und Freiheiten der betroffenen Personen ausgeschlossen werden.

Notwendig ist eine fachliche Diskussion, was eine geforderten Datenschutz-Folgenabschätzung (Art. 35) und eine bisherige Vorabkontrolle gemäß § 4d Abs. 5 BDSG unterscheidet. Denn die bisherige Vorabkontrolle ist an die Verwendung der Art besonderer Daten gekoppelt (§ 3 BDSG Abs. 9). Eine Klassifizierung besonderer Daten in Art. 9 DS-GVO gibt es, die aber keine Erwähnung in Art. 35 findet.

Innerhalb der Datenschutz-Folgenabschätzung ist in Absprache zwischen Verantwortlichen und Aufsichtsbehörden ggf. zu klären, welche Maßnahmen zu ergreifen sind um datenschutzkonforme Verfahren mit der entsprechenden IT bereitzustellen. In den Erwägungsgründen ist durch diverse Beispiele konkretisiert, für welche Anwendungen eine Datenschutz-Folgenabschätzung erforderlich ist, wie optoelektronische Vorrichtungen (Erwägungsgrund 91). Gleichzeitig fällt nur in Erwägungsgrund 91 zur Realisierung von Maßnahmen der gängige Begriff „nach Stand der Technik“. Stattdessen sind Maßnahmen gemäß Art. 35 zu ergreifen, wenn für die betrachteten Verfahren neue Technologien eingesetzt werden. Damit bleibt in großen Teilen unberücksichtigt, dass mehrheitlich kleinere Änderungen in einer ingenieursmäßig betriebenen IT

schrittweise zu Verbesserungen führen, die irgendwann eine Veränderung eines Geschäftsbereichs bewirken können. Einige Kriterien zur Bewertung, ob zu ergreifende Maßnahmen geeignet sind, finden sich z.B. in Art. 32 „Sicherheit in der Verarbeitung“, aber es gibt keine Referenz in Art. 35 auf Art. 32.

Der nationale Gesetzgeber ist aufgefordert nutzbare Regelungen zu treffen, so dass zwischen anwendbaren Schutzbedarfsklassen ein Bezug zum genannten hohen Risiko hergestellt werden kann, insbesondere weil der Begriff des hohen Risikos in der DSGVO nur unzureichend festgelegt ist. Des Weiteren ist eine Transformation in bewährte Begriffe von z.B. Zutritts-, Zugangs-, Zugriffs- oder auch Dokumentationskontrolle anzustoßen. Damit ist eine Lücke zwischen sehr konkreten, technischen Beschreibungen aus den Erwägungsgründen und den abstrakten Prinzipien zu schließen, damit diejenigen, die entsprechende Realisierung in und mit der IT zu verantworten haben, weiterhin eine Anleitung erhalten, an der sie sich orientieren können.

5. Betrieblicher Datenschutzbeauftragter

Die Verankerung des betrieblichen Datenschutzbeauftragten (DSB) in der DSGVO gelang erst im letzten Moment. Die Benennung eines DSBs ist weiterhin vorgesehen. Die Regelungen hierzu sind in Artt. 37, 38 und 39 zu finden. Art. 37 differenziert zwischen den Fällen, in denen auf jeden Fall ein DSB zu benennen ist und denen, in denen es dem europäischen und den nationalen Gesetzgebern überlassen bleibt, Regelungen zu treffen. Nach Art. 37 Abs. 4 können ein Verantwortlicher oder der Auftragsverarbeiter oder Verbände und andere Vereinigungen, die Kategorien von Verantwortlichen oder Auftragsverarbeitern vertreten, einen Datenschutzbeauftragten benennen, es sei denn ein Mitgliedsstaat schreibt die Benennung ausdrücklich vor. Diese Öffnungsklausel sollte der nationale Gesetzgeber in jedem Fall nutzen.

Der DSB darf wegen der Erfüllung seiner Aufgaben nicht abberufen oder benachteiligt werden (Art. 38 Abs. 3). Dieser Abberufungsschutz bleibt hinter den detaillierteren Regelungen im BDSG zurück, das ausdrücklich die Gründe für eine außerordentliche Kündigung fordert. Hier sollte geprüft werden, ob der Gesetzgeber klärend tätig werden kann.

6. Geldbußen und effektive Sanktionen

Die DSGVO stärkt die Befugnisse der Aufsichtsbehörden. In den Artt. 83 Abs. 7, 84 Abs. 1 und Erwägungsgründen 150 sowie 152 öffnet die DSGVO dem nationalen Gesetzgeber Raum für den Erlass von Vorschriften. Der Bund und die Länder können in ihrem Zuständigkeitsbereich festlegen, ob und in welchem Umfang gegen Behörden und öffentliche Stellen, die in dem betreffenden Mitgliedstaat niedergelassen sind, Geldbußen verhängt werden können.

Es obliegt auch den Mitgliedstaaten, Vorschriften über andere Sanktionen für Verstöße gegen die DSGVO festzulegen und alle zur Anwendung erforderlichen Maßnahmen zu treffen. Die DSGVO gibt für diese Sanktionen in Erwägungsgrund 152 nur vor, dass sie wirksam, verhältnismäßig und abschreckend sein müssen. Die Anwendung des kartellrechtlichen Unternehmensbegriffs erfordert eine nationale Anpassung im Ordnungswidrigkeitenverfahren.

7. Beschäftigtendatenschutz

Spätestens mit der DSGVO ist der nationale Gesetzgeber gefordert, ein Beschäftigtendatenschutzgesetz zu verabschieden (Art. 88 i.V.m. Erwägungsgrund 155). Mindestens sind §§ 3 Abs. 11, 32 BDSG beizubehalten.

Douwe Korff*

Privacy seals in the new EU General Data Protection Regulation: Threat or facilitator?

Part 2: What has it turned out to be?

1. The issues

In DANA 3/2015, I compared the proposals for the use of data protection seals in the different versions of the General Data Protection Regulation then under discussion: the original Commission version, the version adopted by the European Parliament, and the Council version. I noticed that while the Commission text “encouraged” the establishment of data protection seal schemes, it added little detail, but that Parliament envisaged a significant role for such seals, allowing them to “demonstrate compliance” by the seal-holder with the requirements for processors (also if the seal-holder were to be a non-EU entity) and similarly to “demonstrate” that “appropriate safeguards” were in place to allow the transfer of personal data

covered by a seal to take place *without further checking by any data protection authority*. Clearly, such seals would be very valuable, especially also in a transnational context, and to non-EU controllers and processors including "cloud" processors.

I warned that such a scheme could only be acceptable if the seals were issued by data protection authorities and if the decision to award a seal would therefore be subject to the "cooperation-", "mutual assistance-" and "consistency" mechanisms included in the Regulation. That way, the proposed issuing of a seal by any one DPA could be challenged by any other DPA in the EU if the processing to be covered by the seal would affect data subjects in the other DPA's Member State; and the seal would in such cases only be issued if there was agreement that that would be appropriate. If on the other hand seals could be issued by entities other than DPAs, to which the issuing of seals was "outsourced" – as was proposed in the version of the Regulation adopted by the Council – then the issuing of seals might not constitute a "measure" taken by a DPA, and might thus not be subject to the consistency mechanism. I wrote that if that road was followed, such "outsourced" seal schemes would pose a serious threat to the new EU data protection framework, effectively creating a massive loophole through which data could be transferred to non-EU processors (including "cloud" processors) and controllers in non-EU countries without adequate data protection, without the DPAs being able to intervene in an effective manner.

These matters were among the many subject matters discussed in the "trilogues" in which the final text of the Regulation was thrashed out between representatives of the Commission, Parliament and the Council. So what does the final, now adopted text say on these issues? As I shall show below, it amounts to a somewhat uneasy, ambiguous compromise.

2. Privacy seals can be issued by "outsourced" certification bodies

The Regulation stipulates that in a number of respects a data protection seal ("certification") can be used as "an element by which to demonstrate" relevant matters, i.e.: general compliance with the obligations imposed on a controller (Art. 24(3)); Privacy-by-Design and -Default (Art. 25(3)); the existence of "sufficient guarantees" for processors (Art. 28(5)); and compliance with data security requirements (Art. 32(3)). In all these cases, the phrase "an element by which to demonstrate" must presumably be read as the creation of a rebuttable presumption: seals can be used as part of the evidence to show compliance in these regards – but they do not in and of themselves prove such compliance. In these respects, therefore, data protection seals are useful, but not conclusive of compliance.

However, in one context this is different: in relation to transfers of personal data to third countries without adequate data protection. Such transfers are in principle prohibited, subject to a limited number of exceptions, including where "appropriate safeguards" are provided by the controller or processor (Art. 46). In the final text of the Regulation, this article stipulates that such appropriate safeguards "may be provided for" *inter alia* by

> an approved certification mechanism pursuant to Article 42 together with binding and enforceable commitments of the controller or processor in the third country to apply the appropriate safeguards, including as regards data subjects' rights (Art. 46(2)(f))

In other words, in this context the seals are conclusive: they provide, in and by themselves, the required safeguards. Indeed, the article adds that certifications can achieve this "**without requiring any specific authorisation from a supervisory authority**" (leading sentence to Article 46(2)).

This threatens to create, in this most highly contentious area, the very danger I warned of in DANA 3/2015, because the final text also provides for the possibility suggested by the Council of data protection seals ("certifications") being issued either by a data protection authority or by a separate "certification body" (Art. 42(5)). In other words, Member States may decide to "outsource" the issuing of the seals, as proposed by the Council.

In that latter case, the certification body must be accredited either by the relevant DPA or by a national accreditation body (or by both) (Art. 43(1)), on the basis of criteria approved by the relevant DPA (Art. 42(5)). Moreover, the approving of the criteria to be applied in accrediting an "outsourced" certification body is subject to the obtaining of an opinion from the new European Data Protection Board (Art. 64(1)(c)), and thus to the consistency mechanism: DPAs must inform the other DPAs of the proposed criteria; they can then exchange views on them and challenge them; and if no agreement can be reached, the matter can be referred to the new European Data Protection Board, which will have the final say (Article 63ff.). Indeed, the Board can in this way adopt certification criteria at the European level which can then (also) become the basis for centrally issued European Data Protection Seals (Art. 42(5)).

But until this is done, it would appear that such "outsourced" seals can in and by themselves constitute the basis for data transfers to third countries without data protection. They can in effect be an alternative to the Safe Harbor, or its contentious proposed successor, the "EU-US Privacy Shield", and to the use of standard or ad hoc data transfer contract clauses. In my opinion, this should mean that they should be subject to broad overall EU-level control.

3. Can seals be challenged?

If any processing to be covered by a seal relates only to the activities of a controller established in one Member States and if it does not substantially affect (and is unlikely to substantially affect) data subjects in any other Member State, the matter is almost entirely left to the DPA or certification body in question, without involvement of any other DPA (although if such seals were to be used to allow transfers of data originating from other Member States that would not be allowed directly from those other Member States, the DPAs of those other Member States would probably be able to demand action from the DPA in the Member State where the seal was issued, even if this was "outsourced").

However, if the processing to be covered by a seal involves:

> processing of personal data which takes place in the context of the activities of establishments in more than one Member State of a controller or processor in the Union where the controller or processor is established in more than one Member State –

or if it involves:

> processing of personal data which takes place in the context of the activities of a single establishment of a controller or processor in the Union but which substantially affects or is likely to substantially affect data subjects in more than one Member State –

then the matter is regarded as "cross-border processing" (Art. 4(23(a) and (b)). In that case, any decisions or measures relating to the processing, proposed or drafted by the relevant "lead supervisory authority", are subject to the "cooperation-", "mutual assistance-" and "consistency mechanisms" in the Regulation.

If, in a particular Member State, the DPA (or DPAs) are charged with issuing data protection seals, then clearly the issuing of such seals constitute the taking of "decisions" or "measures" by such DPAs. If a (proposed or draft) decision to issue a seal relates to such cross-border processing, and such a seal-issuing DPA is the "lead supervisory authority" in respect of it, then (because this is a proposed or draft decision that relates to cross-border processing) that DPA must inform the DPAs in any other Member State affected by the processing (Art. 60(1)); may ask them to assist in the evaluation and certification process (Art. 60(2)); and must in any case:

> without delay, communicate the relevant information on the matter to the other supervisory authorities concerned [and] without delay submit a draft decision [here: on whether to award the seal] to the other supervisory authorities concerned for their opinion and take due account of their views. (Art. 60(3))

If any of those other authorities:

> within a period of four weeks after having been consulted in accordance with paragraph 3 of this Article, expresses a relevant and reasoned objection to the draft decision, the lead supervisory authority shall, if it does not follow the relevant and reasoned objection or is of the opinion it is not relevant and reasoned, submit the matter to the consistency mechanism … (Art. 60(4))

Under this mechanism, the European Data Protection Board must then adopt a binding decision on the matter (Art. 65(1)(a)). In other words, in such cases the Board will have the final say on whether the proposed seal can be issued or not.

The issue is more complicated when seals are issued by "outsourced" certification bodies, because the issuing of seals by such "outsourced" bodies does not, as such, constitute acts of the DPA in the Member State concerned.

However, the compromise text could still offer some ways of referring the matter to the new Board.

First of all, the final text of the Regulation contains a new power that must be granted to DPAs, not envisaged in any of the draft texts (and presumably aimed at countering the very threat I noted in DANA 3/2015 of "outsourced" seals opening up loopholes in protection). Article 58(2)(h) stipulates that all DPAs must be granted the power:

> to withdraw a certification or to order the certification body to withdraw a certification issued pursuant to Articles 42 and 43, or to order the certification body not to issue certification if the requirements for the certification are not or are no longer met.

Although it is oddly not spelled out in the Regulation, it is implicit in the above, and in the duty of the EDPB to collate all seals issued (Article 43(6)), that "outsourced" certification bodies should at least inform their national DPA of any seals they issue (or intend to issue), and that those DPAs must then inform all other DPAs and the EDPB of them.

One could argue that a decision by a DPA to not use this power should be regarded as a decision subject to the "cooperation-", "mutual assistance-" and "consistency mechanisms" – especially if a DPA specifically informs the other DPAs and the Board of such unopposedly-issued seals. Such informing can, I believe, be seen as at least a tacit endorsement of the reported seal.

In any case, the duty to apply the "cooperation-", "mutual assistance-" and "consistency mechanisms" are drafted in broad terms, not necessarily limited to cases of specific "decisions" or "measures" or "complaints" and "investigations" (although they clearly focus on those). Thus, Article 60, which establishes the cooperation mechanism, can be read as applying to any matter involving a lead supervisory authority and one or more other supervisory authorities concerned, i.e., to all cross-border processing issues (cf. the absence of any references to "decisions" in Article 60(1) and the very general reference in Article 60(3) to "the matter" under consideration). Mutual assistance also has the aim, quite generally, "to implement and apply this Regulation in a consistent manner" (Art. 61(1)). The fact that this mechanism applies "in particular [to] information requests and supervisory measures" does not mean that it does not also extend to the use of the power in Article 58(2)(h). And the consistency mechanism, as its name already makes clear, is also quite broadly aimed at "contribut[ing] to the consistent application of this Regulation throughout the Union" (Art. 63).

Arguably, therefore, in countries in which the issuing of data protection seals is "outsourced", the lead DPA must still inform other concerned DPAs of any seal that an "outsourced" certification body wants to issue or has issued (or better: of any seal application) relating to cross-border processing, even if the lead DPA in question is not in direct charge of the seal issuing. That lead DPA must then also cooperate with the other concerned DPAs on the question of whether to exercise its power to prevent the issuing of the seal (or to order its withdrawal). And if the lead DPA refuses to do this, other DPAs should be able to challenge the seal – technically: the refusal of the lead DPA to use these powers in respect of the seal – in the EDPB, which must have the final say.

However, given the ambiguities in the text of the Regulation, this view can

only be tentative.

4. The solution

Given that "outsourced" data protection seals that are not subject to the "cooperation-", "mutual assistance-" and "consistency mechanisms" can pose grave risks to the fundamental rights of EU data subjects, it is important that the matters discussed above be clarified as a matter of urgency.

The best option would, in my view, be to leave the final decision on whether to issue a seal in all cases to the relevant DPA (in both purely domestic and cross-border cases). That would not stand in the way of outsourcing much of the "frontline" work. The evaluation of the relevant product or service could still be done by approved independent experts; and bodies such as the certification bodies mentioned could still be tasked with the checking of those evaluations and the preparation of the seals. However, those would only be provisional seals: in order to come into effect, they would need to be endorsed by the relevant DPA – and that endorsement would constitute an act (decision, measure) of that DPA and would thus be subject to the "cooperation-", "mutual assistance-" and "consistency mechanisms".

Alternatively, if some countries are adamant that they want to fully and formally outsource the issuing of seals, they should still accept that if they inform their fellow-DPAs in the other Member States and the EDPB of any shortly-to-be-issued "outsourced" seal that relates to a product or service that involves cross-border processing of personal data, this constitutes a decision by them not to prevent the issuing of the seal or to order the withdrawal of the seal; and that that (negative) decision is subject to the "cooperation-", "mutual assistance-" and "consistency mechanisms". This could be agreed, e.g., in the Article 29 Working Group pending the fully entering into force of the Regulation, or by the EDPB as soon as it is established.

Without such clarification, the matter remains ambiguous and, in relation to data protection seals, problematic.

In the somewhat longer term, the establishment of a European Data Protection Seal for products or services involving cross-border processing of personal data, operating under the aegis of the European Data Protection Board (rather than any individual DPA), would be the better option still.

* Douwe Korff is Emeritus Professor of International Law at London Metropolitan University, Associate of the Oxford Martin School of the University of Oxford, and Fellow at the Centre for Internet and Human Rights of the European University of Viadrina, Frankfurt/O. and Berlin.

Peter Schaar

Europäischer Datenschutz: Ende gut, alles gut?

Nachdem das Reformpaket die letzten Hürden genommen hat, müsste man eigentlich erleichtert aufatmen. Die Datenschutz-Grundverordnung hat den Trilog von Rat, Kommission und Parlament überraschend gut überstanden. Auch die überzeugenden Voten im Europäischen Parlament und im Rat waren ein deutliches Signal für die Handlungsfähigkeit Europas beim Datenschutz – eine Handlungsfähigkeit, die man derzeit in anderen Bereichen, etwa der Flüchtlings- und Finanzpolitik, schmerzlich vermisst.

Wesentliche Elemente der von der Kommission angestoßenen Reform, die während des mehr als vierjährigen Verhandlungsmarathons immer wieder in Frage gestellt worden waren, blieben erhalten oder wurden sogar gegenüber dem Entwurfstext stärker akzentuiert. Dies gilt etwa für die Ausdehnung des Anwendungsbereichs auf Anbieter elektronischer Dienste mit Sitz in einem Drittland („Marktortprinzip", Art. 3 Abs. 3 DS-GVO) oder die sehr deutliche Verschärfung der Sanktionen bei Datenschutzverstößen (Art. 83). Auch die Forderungen nach einer radikalen Aufweichung der Zweckbindung personenbezogener Daten blieben im Ergebnis erfolglos ebenso wie der Versuch, den Anwendungsbereich der europäischen Vorschriften drastisch einzuschränken.

Die Europäische Union hat also die (rechtlichen) Herausforderungen an das Datenschutzrecht angenommen und Konflikte zunächst durchgestanden. Die EU-weite Harmonisierung des Datenschutzrechts erfolgt auf verhältnismäßig hohem Level und schreibt nicht bloß einen kleinsten gemeinsamen Nenner fest.

Durchaus ambivalent ist es hingegen, dass der Verordnungstext den Mitgliedstaaten erhebliche Gestaltungsmöglichkeiten belässt. Dies eröffnet den nationalen Gesetzgebern zum einen die Chance, in bestimmten Bereichen über die in der Verordnung europaweit festgeschriebenen Mindeststandards hinauszugehen bzw. diese zu konkretisieren. Dies ist der Fall etwa beim Schutz von Gesundheitsdaten (Art. 9 Abs. 4 lit. a), beim Beschäftigtendatenschutz (Art. 88) und dies gilt auch für die Regelungen zur obligatorischen Benennung betrieblicher Datenschutzbeauftragter (Art. 37). Andererseits ist zu befürchten, dass die nationalstaatlichen Regelungsspielräume auch dazu herhalten müssen, bestehende Datenschutz-Schwachstellen beizubehalten – etwa das deutsche Meldegesetz, das eine generelle Meldepflicht mit sehr freizügigen Übermittlungsmöglichkeiten ohne angemessene Zweckbindung kombiniert. Auch in anderen Mitgliedstaaten gibt es solche fragwürdigen Bestimmungen, die so eine zweite Chance bekommen haben.

Die Konferenz der Datenschutzbeauftragte des Bundes und der Länder hat jüngst gefordert, die von der Datenschutz-Grundverordnung eingeräumten nationalen Spielräume im Sinne eines möglichst hohen Datenschutzniveaus zu nutzen. Wem an einem starken deutschen Datenschutz gelegen ist, der kann

diese Position nur unterstützen. Manche Äußerungen von Regierungsvertretern, etwa von Bundeswirtschaftsminister Gabriel und Bundesverkehrsminister Dobrint gegen die angeblich weltfremde und wirtschaftsfeindliche Maxime der „Datensparsamkeit" lassen aber befürchten, dass in dieser Frage noch ein hartes Ringen bevorsteht.

Neues Zwei-Phasen-Modell?

Das Bundesinnenministerium hat inzwischen angekündigt, die erforderlichen Änderungen des deutschen Rechts in einem Zwei-Phasen-Modell zu realisieren. In einem ersten Schritt sollen die unbedingt erforderlichen Gesetzesänderungen erfolgen; in einem zweiten Schritt sollen dann weitere Anpassungen stattfinden. Zu der ersten Phase soll die Ausgestaltung der Befugnisse der Datenschutzaufsichtsbehörden und die Einpassung ihrer Sanktionsbefugnisse ins deutsche Rechtssystem gehören (Artt. 51-59), auch im Hinblick auf den Rechtsschutz der Betroffenen und die gerichtliche Überprüfung der Aufsichtsmaßnahmen. Unbedingt erforderlich ist es auch, die Zusammenarbeit der deutschen Datenschutzbehörden und die Außenvertretung des deutschen Datenschutzes im neu einzurichtenden Europäischen Datenschutzausschuss zu klären. Die Gesetzgebungskompetenz für derartige Zuständigkeitsfragen liegt jedoch nicht ausschließlich beim Bund. Vielmehr muss hier eine gemeinsame Rechtsvorschrift von Bund und Ländern erlassen werden, etwa in Form eines noch auszuhandelnden Staatsvertrags. Schließlich gehört noch die Ausgestaltung des Verhältnisses von Datenschutz einerseits und der Freiheit der Meinungsäußerung und Informationsfreiheit andererseits (Art. 85 DS-GVO) zum Pflichtprogramm.

Das vom Bundesinnenministerium angekündigte Phasenmodell löst bei mir negative Assoziationen aus, erinnert es doch an die im Jahr 2000 ebenfalls in zwei Phasen angekündigte grundlegende Modernisierung des deutschen Datenschutzrechts: Nahezu sämtliche angekündigten, etwas ambitionierten Änderungen blieben dabei auf der Strecke, denn die versprochene zweite Phase hat es nie gegeben. Auch damals saßen die Erfinder im Bundesinnenministerium.

Kompetenzfragen als Machtfragen

Bekanntlich gehören Kompetenzfragen zu den am schwierigsten zu lösenden Problemen. Anders als die bisherige Artikel-29-Gruppe wird der Europäische Datenschutzausschuss (Artt. 60-67) im Falle eines Dissenses zwischen Datenschutzbehörden entscheiden. Dagegen bleibt es den Mitgliedstaaten überlassen, die jeweiligen Zuständigkeiten und die Außenvertretung der Datenschutzbehörden abzugrenzen, wenn – wie in Deutschland – mehr als eine Datenschutzbehörde eingerichtet wurde.

Eine Weile hatte man den Eindruck, Datenschutz sei aus Sicht der Politik ein gestriges Thema, von dem man sich am besten fern hält. Seit einiger Zeit hat sich der Wind aber gedreht: Niemand kann heute ernsthaft bestreiten, dass der Datenschutz eng mit der Digitalisierung der gesamten Gesellschaft verbunden ist und dass mit der datenschutzrechtlichen Kompetenzverteilung auch darüber entschieden wird, wer die Weichen in die Informationsgesellschaft stellt.

Das Bundesinnenministerium scheint davon auszugehen, dass die allermeisten datenschutzrechtlichen Spezialgesetze zunächst nicht geändert werden müssen. Ich halte diese Position für risikoreich: Zwar ist es richtig, dass die Grundverordnung für bestimmte Felder, insbesondere im Bereich der staatlichen Datenverarbeitung, weiterhin Regelungsspielräume enthält. Anderseits muss auch in diesen Bereichen die Einhaltung der europäischen Standards gewährleistet sein. Dies gilt zum Beispiel für das Sozialrecht: So sind im zehnten Buch des Sozialgesetzbuchs (SGB X) die derzeitigen Regelungen des Bundesdatenschutzgesetzes praktisch gedoppelt - etwa im Hinblick auf die Anforderungen an die Auftragsdatenverarbeitung. Es ist kaum vorstellbar, dass diese unverändert Bestand haben können, ohne bei den Rechtsanwendern zu unlösbaren Konflikten zu führen. Vergleichbare Konstellationen gibt es auch in vielen anderen Bereichen.

Betrieblichen Datenschutz und Beschäftigtendatenschutz nicht auf lange Bank schieben

Besonders intensiv waren die Diskussionen vor der Verabschiedung der Datenschutzgrundverordnung über die betrieblichen Datenschutzbeauftragten und über den Beschäftigtendatenschutz. In beiden Bereichen haben die Mitgliedsstaaten weiterhin Gestaltungsspielraum.

Bei den betrieblichen Datenschutzbeauftragten hatte die Bundesregierung in letzter Sekunde im Trilog eine nationale Öffnungsklausel (Art. 37 Abs. 4) durchgesetzt, die das derzeitige deutsche Modell großenteils bewahren könnte – vorausgesetzt, eine entsprechende deutsche Bestimmung wird rechtzeitig – vor dem Inkrafttreten der DS-GVO in zwei Jahren – beschlossen. Nimmt man die Absicht des Bundesinnenministeriums beim Wort, zunächst nur das „Unabweisbare" gesetzlich neu zu regeln, dann würden die Regeln zum betrieblichen Datenschutzbeauftragten nicht dazu gehören.

Beim Datenschutz im Beschäftigungsverhältnis (Art. 88) stellt sich nicht nur die Frage nach einem deutschen Beschäftigten-Datenschutzgesetz. Auch die Zukunft der bisherigen Regelung des § 32 BDSG zum Umgang mit Beschäftigtendaten steht zur Disposition. Schon sind aus der Wirtschaft Warnungen zu vernehmen, hier einen „deutschen Sonderweg" einzuschlagen. Es ist leider zu befürchten, dass derartige Meinungsäußerungen in der Politik nicht ohne Wirkung bleiben werden. Angeblich soll es zwischen den Regierungsfraktionen der CDU/CSU und der SPD schon verabredet zu sein, in dieser Legislaturperiode auf ein Beschäftigtendatenschutzgesetz zu verzichten - ein klarer Bruch der Zusagen aus dem Koalitionsvertrag.

vzbv – Florian Glatzner

Datenschutz in Europa: Die roten Linien des vzbv zur europäischen Datenschutz-Grundverordnung – revisited

Nach mehr als vier Jahren Verhandlungen ist die Datenschutz-Grundverordnung der Europäischen Union endlich beschlossen. Insgesamt ist der finale Gesetzestext aus Verbrauchersicht besser ausgefallen, als man es während der Verhandlungen befürchten musste. Trotz Lobbyarbeit bisher unbekannten Ausmaßes von europäischen und US-amerikanischen Wirtschaftsverbänden wurden die Vorschläge der EU-Kommission und des Europäischen Parlaments nicht völlig verwässert. Dennoch enthält die Verordnung auch viele schwache Regelungen, die teilweise zu einer Absenkung des bisherigen Datenschutzniveaus führen könnten, wenn die Mitgliedsstaaten dies nicht über die Ausgestaltung ihrer Spielräume verhindern.

Im Sommer 2015 hatte der Verbraucherzentrale Bundesverband (vzbv) unter anderem in der DANA 3/2015 rote Linien definiert, hinter die die Datenschutz-Grundverordnung nicht zurückfallen dürfe. Dies betraf besonders die umstrittenen Punkte der „Datensparsamkeit“, des „berechtigten Interesses der datenverarbeitenden Stelle“, der „Änderung des Verarbeitungszwecks“ sowie der „Profilbildung“. Auf was hat man sich in diesen Bereichen nun geeinigt?

1. Datensparsamkeit

Eine Datenverarbeitung darf nur in dem Umfang erfolgen, der notwendig ist, um den angestrebten Zweck zu erfüllen. Insbesondere soll der Zeitraum der Datenspeicherung minimiert werden, beispielsweise durch Lösch- und Anonymisierungsfristen oder regelmäßige Überprüfungen, ob die Daten noch notwendig sind.

Hier konnte sich der Rat der Europäischen Union nicht mit seiner Forderung durchsetzen, nach der eine Datenverarbeitung lediglich „nicht exzessiv“ erfolgen sollte, was zu einer deutlichen Absenkung des Datenschutzes geführt hätte. Dementsprechend begrüßt der vzbv die nun verabschiedete Regelung.

2. „Berechtigtes Interesse“ der datenverarbeitenden Stelle

Das berechtigte Interesse eines Unternehmens oder eines Dritten kann Rechtsgrundlage für eine Verarbeitung von personenbezogenen Daten sein, sofern Interessen des Verbrauchers nicht überwiegen und seine vernünftigen Erwartungen, die auf seinem Verhältnis zum Unternehmen beruhen, erfüllt werden. Dies kann zum Beispiel der Fall sein, wenn die betroffene Person ein Kunde des Unternehmens ist.

Als kritisch wertet der vzbv hier, dass „Direktmarketing“ unter Umständen ein berechtigtes Interesse sein kann, für das somit keine Einwilligung notwendig wäre. Stammen Daten – auch sensible persönliche Daten – aus öffentlich zugänglichen Quellen, so dürfen diese auch auf Grundlage des berechtigten Interesses verarbeitet werden.

Insgesamt ist diese Vorschrift noch auslegungsbedürftig, besonders hinsichtlich des neuen Konstrukts der „vernünftigen Erwartungen des Verbrauchers“ – was zu Missbrauch führen könnte.

Positiv hervorzuheben ist, dass der Verbraucher bei der Verarbeitung seiner Daten auf Grundlage eines berechtigten Interesses ein Widerspruchsrecht hat – das gilt auch, falls auf Grundlage eines berechtigten Interesses zur Profilbildung kommt. Legt der Verbraucher Widerspruch ein, muss das Unternehmen darlegen, warum sein Interesse gegenüber dem des Verbrauchers überwiegt.

3. Änderung des Verarbeitungszwecks

Die Änderung des Verarbeitungszwecks ist nur erlaubt, wenn der ursprüngliche Zweck mit dem neuen beziehungsweise veränderten Zweck kompatibel ist. Die Kriterien, die für diese Prüfung herangezogen werden müssen, sind die Verbindung zwischen den Verarbeitungszwecken, der Zusammenhang der Datenerhebung (insbesondere das Verhältnis zwischen dem Unternehmen und dem Verbraucher), die Art der Daten (sind es sensible Daten?), die Folgen für den Verbraucher sowie Sicherheitsmaßnahmen (werden die Daten pseudonymisiert oder verschlüsselt?).

Eine Zweckänderung soll aber auch zu unvereinbaren Zwecken möglich sein, wenn der Verbraucher einwilligt. Eine Weiterverarbeitung soll ferner stets „für im öffentlichen Interesse liegende Archivzwecke, für wissenschaftliche oder historische Forschungszwecke oder für statistische Zwecke“ erlaubt sein.

Problematisch aus Sicht des vzbv ist, dass die Kriterien für die Zweckänderung recht unbestimmt sind und erst noch in der Praxis ihre Wirksamkeit beweisen müssen. Außerdem könnte sich insbesondere der letzte Punkt zu einem Einfallstor für unlautere Praktiken entwickeln: Unter dem Deckmantel der Forschung und Statistik könnten zum Beispiel soziale Netzwerke möglicherweise Experimente zur Beeinflussung der Stimmung ihrer Nutzer oder Suchmaschinen statistische Analysen zu Werbezwecken durchführen.

Insgesamt ist der Abschnitt zur Zweckänderung jedoch besser ausgefallen, als die Position der Mitgliedstaaten es hatte erwarten lassen, da grundsätzlich eine Zweckänderung nur bei einer Vereinbarkeit der Zwecke und nicht

auch bei inkompatiblen Zwecken möglich ist.

4. Profilbildung

Der Verbraucher hat das Recht, keiner automatisierten Einzelfallentscheidung (Profilbildung) zu unterliegen, die rechtliche Wirkung entfaltet oder ihn signifikant beeinträchtigt – es sei denn, es gibt eine gesetzliche Erlaubnis oder sie ist für die Erfüllung eines Vertrags notwendig oder der Verbraucher hat explizit eingewilligt.

Die Bildung von Profilen als solche – und nicht nur die reine Entscheidung, die rechtliche Wirkung entfaltet oder Verbraucher signifikant beeinträchtigt – unterliegt keinem gesonderten Schutz und wird nur als eine „normale" Datenverarbeitung angesehen.

Der Verbraucher hat zwar ein Recht auf menschliche Intervention, Erklärung und Anfechtung der Entscheidung – in der Praxis dürfte das aber nur eine untergeordnete Rolle spielen.

Die Verordnung schreibt vor, dass Unternehmen geeignete mathematische oder statistische Methoden verwenden und Maßnahmen treffen sollen, um Fehler zu minimieren und Diskriminierung aufgrund von Rasse, ethnischer Herkunft, politischer Meinung, Religion oder Weltanschauung, Gewerkschaftszugehörigkeit, genetischer Anlagen oder Gesundheitszustand sowie sexueller Orientierung zu verhindern. Diese Ergänzung findet sich allerdings nur in den Erwägungsgründen der Verordnung, was sie wiederum schwächt.

Insgesamt befürchtet der vzbv an dieser Stelle eine Absenkung des Verbraucherschutzes im Vergleich zum deutschen Status Quo. Bisher war etwa Kreditscoring alleine auf der Grundlage von Adressdaten nicht erlaubt – was sich nun ändern könnte. Auch wäre es künftig möglich, dass auch bestrittene Forderungen an Auskunfteien gemeldet werden. Dies könnte dazu führen, dass Verbraucher nur aus Angst vor den negativen Auswirkungen eines schlechten Scorewertes gegenüber Forderungsgebern einlenken und die Forderung akzeptieren.

In der Vergangenheit hatte die Bundesregierung stets betont, dass der bestehende deutsche Datenschutzstandard durch die Datenschutz-Grundverordnung nicht abgesenkt werden dürfe. Die Beispiele zeigen jedoch, dass das bisherige deutsche Daten- und Verbraucherschutzniveau im Bereich des (Kredit-)Scorings allein durch die Datenschutz-Grundverordnung nicht beibehalten wird. Sollte die Bundesregierung dem nicht noch in dieser Legislaturperiode entgegen wirken, würde dies erneut zu jahrelangen Rechtsunsicherheiten für Verbraucher und Unternehmen führen, die gerade erst im Jahr 2009 durch die Novelle des Bundesdatenschutzgesetztes ausgeräumt wurden.

Daher sollte die Bundesregierung die Möglichkeiten der in der Verordnung vorgesehenen Öffnungsklauseln konsequent ausschöpfen sowie alle weiteren rechtlichen Spielräume ausnutzen, um das deutsche Datenschutzniveau im Bereich des (Kredit-)Scorings zu erhalten. Insbesondere sollte auch geprüft werden, ob bestimmte Regelungsinhalte des Bundesdatenschutzgesetzes, wie die Bestimmungen des § 28b BDSG, in andere Gesetze mitaufgenommen werden können. Denkbar wären beispielsweise Regelungen im Zivil-, Vertrags- und Versicherungsrecht sowie im Kreditwesengesetz, die festlegen, unter welchen Umständen Scorewerte verwendet werden dürfen, und die Vorgaben zur Sicherung der Datenqualität machen.

Werner Hülsmann

Gestaltungsspielräume für die Nationalstaaten und Planungen des Bundesministeriums des Inneren

Regelungsräume – aber keine Öffnungsklausen

Thomas Zerdick, stellv. Leiter des Referat C.3 Schutz personenbezogener Daten der Generaldirektion Justiz und Verbraucher in der Europäische Kommission, stellte am 09. Juni 2016 anlässlich einer Veranstaltung der Europäischen Akademie für Informationsfreiheit und Datenschutz (EAID) klar: „Es gibt keine ‚Öffnungsklauseln‘, sondern ‚Konkretisierungsklauseln‘, die ‚Einräumung von Optionen‘, ‚Ausnahmevorschriften‘ und ‚Regelungsaufträge‘ also ‚Regelungsräume‘“. Diese Regelungsräume können – und müssen zum Teil – von den Mitgliedstaaten genutzt werden. Das Inkrafttreten der Datenschutzgrundverordnung am 25. Mai 2016 führte laut Zerdick dazu, dass die Mitgliedstaaten keine rechtlichen Regelungen mehr erlassen dürfen, die gegen diese Verordnung verstoßen.

Zu den **Konkretisierungsklauseln** gehört Art. 6 Abs. 1 Buchstaben c und e.

Optionen werden den Mitgliedstaaten eingeräumt durch

- EWG 27: Mitgliedstaaten können Regelungen zu Daten von Verstorbenen festlegen, wie es sie derzeit in Deutschland im Sozialgesetzbuch (SGB) gibt
- Art. 8 – Bedingungen für die Einwilligung eines Kindes in Bezug auf Dienste der Informationsgesellschaft: Mitgliedstaaten können die Altersgrenze bis auf 13 Jahre herunterfahren
- Art. 37 Abs. 4: Mitgliedstaaten können Regelungen zur Verpflichtung zur Bestellung von betrieblichen Datenschutzbeauftragten erlassen
- Art. 80 – Vertretung von betroffenen Personen: Mitgliedstaaten können Regelungen zum Klagerecht von Vereinen bei Datenschutzverstößen erlassen oder beibehalten. Ein solches ist in Deutschland inzwischen im Verbandsklagerecht eingefügt
- Art. 83: Ermöglicht es den Mitgliedstaaten Bußgelder für Datenschutzverstöße durch öffentliche Stellen festzulegen
- Art. 88: Beschäftigtendatenschutz: Die Mitgliedstaaten können spezielle, konkretisierende Regelungen erlassen, diese dürfen aber nicht gegen die DSGVO verstoßen, auch Betriebsvereinbarungen und Tarifverträge mit Regelungen zum Beschäftigtendatenschutz sind weiterhin möglich

Zu den Bereichen, in denen **Ausnahmeregelungen** möglich sind, gehören:

- Art. 21: Widerspruchsrecht
- Art. 89: Garantien und Ausnahmen in Bezug auf die Verarbeitung zu im öffentlichen Interesse liegenden Archivzwecken, zu wissenschaftlichen oder historischen Forschungszwecken und zu statistischen Zwecken, Absätze 2 und 3 ermöglichen es Mitgliedstaaten, Regelungen für den Bereich der wissenschaftlichen und historischen Forschung sowie zu Archivzwecken zu schaffen

Regelungsaufträge an die Mitgliedstaaten sind

- Kapitel VI: Die Mitgliedstaaten müssen konkrete Regelungen zu den Datenschutzaufsichtsbehörden festlegen
- Art. 84: Sanktionen: Die Mitgliedstaaten sollen festlegen, ob und wenn ja, für welche Datenschutzverstöße z.B. Straftatbestände geschaffen werden
- Art. 85 Verarbeitung und Freiheit der Meinungsäußerung und Informationsfreiheit: Hier sollen Mitgliedstaaten Regelungen schaffen, die „das Recht auf den Schutz personenbezogener Daten gemäß dieser Verordnung mit dem Recht auf freie Meinungsäußerung und Informationsfreiheit, einschließlich der Verarbeitung zu journalistischen Zwecken und zu wissenschaftlichen, künstlerischen oder literarischen Zwecken, in Einklang“ bringen

Fahrplan der EU-Kommission

In den nächsten zwei Jahren will sich die EU-Kommission laut Zerdick informieren, Kontakte zu Verbänden aufnehmen sowie die Umsetzung der EU-Datenschutzrichtlinie für Polizei und Justiz begleiten. Am 28./29. Juli 2016 findet eine gemeinsame Veranstaltung mit der Art. 29 Gruppe zur Auslegung und Umsetzung der DS-GVO statt. Darüber hinaus ist auch eine Anpassung von EU-Recht an die DSGVO erforderlich. So soll u.a. die E-Privacy-Richtlinie überarbeitet werden. Eine Überarbeitung der EU-Richtlinie zum elektronischen Geschäftsverkehr sei nicht erforderlich, da die DSGVO vollumfänglich im elektronischen Geschäftsverkehr gilt und diese Richtlinie daher zum 25. Mai 2018 überflüssig werde.

Auf Nachfrage erläuterte Zerdick, dass die EU-Kommission die Durchführungs- und delegierten Rechtsakte als Möglichkeit für die Kommission aber nicht als Verpflichtung ansehe und daher erst einmal abwarten werde, was die Datenschutzaufsichtsbehörden und der EU-Datenschutzausschuss an Vorgaben erarbeite.

Nach Ansicht von Zerdick seien Lokaliserungsvorschriften, wie sie beispielsweise z.Zt. im SGB bestehen, mit dem Wirksamwerden der EU-Richtlinie nicht mehr zulässig. Diese Auffassung wurde allerdings von anwesenden ehemaligen Bundes- und Landesdatenschutzbeauftragten kritisch gesehen, da dann eine Beschränkung der Verarbeitung der sehr sensiblen Sozialdaten auf Dienstleister mit Sitz in Deutschland nicht mehr möglich wäre.

Planungen des Bundesministeriums des Inneren

Das Bundesministerium des Inneren plant die Umsetzung der Regelungsräume in zwei Paketen. Das eine Paket mit den Regelungen, die zum einen nach der DSGVO erforderlich sind und zum anderen wünschenswert und politisch einfach umsetzbar sind, soll noch bis zum Frühjahr 2017, also vor dem Bundestagswahlkampf im nächsten Jahr, verabschiedet werden. Der Zeitplan ist eng, da auch die Bundesländer – insbesondere wegen den zu treffenden Regelungen zu den Datenschutzaufsichtsbehörden – beteiligt werden müssen. Ein erster Referentenentwurf soll vorliegen, die Ressortabstimmung bereits begonnen haben. Bei Redaktionsschluss lag der Entwurf allerdings noch nicht öffentlich vor. Das zweite Paket ist erst für die Zeit nach der Bundestagswahl vorgesehen. Ob – und wenn ja, wann – es kommt ist daher derzeit noch nicht vorhersehbar.

Paket 1

Jörg Eickelpasch, Referat V II 4 – Datenschutzrecht beim Bundesministerium des Innern (BMI) führte bei der EAID-Veranstaltung die Pläne der Bundesregierung, insbesondere die des BMI, aus. Geplant ist ein Artikelgesetz (als Arbeitstitel hierfür wurde schon mal „BDSG-Ablösegesetz“ genannt). Darin soll ein Artikel das derzeitige Bundesdatenschutzgesetz zum 25. Mai 2018 aufheben. Mit einem weiteren Artikel soll ein neues Datenschutzgesetz geschaffen werden, das sich von seiner Struktur her an der DSGVO orientieren wird. Das neue Datenschutzgesetz soll laut Eickelpasch die folgenden Elemente enthalten.

Kapitel 1 - Allgemeine Vorschriften

Das BDSG gilt auch für Bereiche, für die die DSGVO nicht gilt, z.B. für Strafverfahren, daher bedarf es Regelungen zur Anwendbarkeit des neuen Gesetzes. Die Bestellpflicht von Datenschutzbeauftragten soll auch hier zu finden sein. Dabei sollen die bisherigen Regelungen aus dem § 4f BDSG bezüglich der Verpflichtung zur Bestellung erhalten bleiben. Leider gibt es Stimmen aus dem Bundesministerium der Wirtschaft, die zumindest die Anzahl der Personen, ab der eine Bestellung eines Datenschutzbeauftragten verpflichtend sein soll, deutlich erhöht sehen wollen.

Kapitel 2

Hier soll durch Nutzung von Art. 22 Abs. 2 Buchstabe b die Regelung aus § 6a BDSG erhalten bleiben, dass automatisierte Einzelentscheidungen auch dann zulässig sein sollen, wenn sie Vorteile für den Betroffenen bringen.

Kapitel 3: Rechte der Betroffen

Hier sollen nach Auffassung des BMI die Möglichkeiten des Art. 23 Beschränkungen genutzt werden.

Kapitel 4: Aufsichtsbehörden

Hier sind auf Bundesebene Regelungen zur Wahl und Rechtstellung des/der Bundesbeauftragten für den Datenschutz und die Informationsfreiheit zu treffen. Weiterhin soll das Recht der Aufsichtsbehörden auf Klagebefugnis gegen Angemessenheitsbeschlüsse der EU-Kommission eingeführt werden.

Kapitel 5: Zusammenarbeit und Kohärenz

Als zentrale Anlaufstelle soll die BfDI eingerichtet werden. Zur Vertretung im EU-Datenschutzausschuss stellt sich die Frage, wer dies überhaupt regeln darf. Es wird derzeit nach einer einvernehmlichen Lösung zwischen Bund, Ländern und Datenschutzaufsichtsbehörden gesucht. Ebenfalls sind Regelungen zur federführenden Aufsichtsbehörde zu treffen.

Kapitel 6: Besondere Datenverarbeitungen

Dieses Kapitel soll insbesondere enthalten:

- Auf Basis von Art. 85 Regelung zur Deutschen Welle
- Regelungen zum Beschäftigtendatenschutz, gedacht ist an eine Übernahme von § 32 BDSG (vgl. Art. 88)
- Datenverarbeitung zu privilegierten Zwecken (wissenschaftliche Forschung, Statistik, Archive, vgl. Art. 89)
- Regelungen zur Datenverarbeitung von Auskunftdateien. Dabei soll versucht werden die Regelungen des bisherigen § 28a BDSG zu erhalten. Dies wird von der Wirtschaft, den Verbraucherschutzverbänden und der Mehrheit der Datenschutzaufsichtsbehörden gewünscht. Falls dies nicht möglich sein sollte, wäre hier die DSGVO anzuwenden, das würde allerdings zu Rechtsunsicherheit führen. Derzeit werden drei Ideen zum Erhalt der Regelungen des § 28a BDSG erörtert: a) Nutzung von Art. 6 Abs. 4 i.V.m. Art. 23 Abs. 1, b) es handelt sich hierbei gar nicht um Datenschutzrecht, sondern um Gewerberecht oder c) „öffentliches Interesse“. Eine konkrete Begründung, warum dieser Regelung im öffentlichen Interesse sei, konnte Herr Peickenpasch leider noch nicht angeben.
- Datenverarbeitung der Berufsgeheimnisträger, hier argumentiert das BMI, dass ein uneingeschränktes Auskunftsrecht dazu führen könne, dass Berufsgeheimnisträger ihr Berufsgeheimnis gegenüber Mandaten verletzen müssten. Auch das Recht der Datenschutzaufsichtsbehörden, jederzeit in alles Einsicht zu nehmen, müsse bei Berufsgeheimnisträgern aus diesem Grund eingeschränkt werden. Dies wird allerdings von Datenschutzverbänden und Aufsichtsbehörden kritisch gesehen!

Kapitel 7 Schadenersatz, Bußgeldvorschriften und Strafvorschriften

In diesem Kapitel sollen Regelungen zum Schadenersatz, konkretisierende Regelungen zu Bußgeldvorschriften, soweit diese nach der DSGVO zulässig sind, und zu Strafvorschriften, soweit solche erforderlich sind, enthalten sein.

Paket 2

Da das zweite Paket frühestens nach der 2017 stattfindenden Bundestagswahl kommen wird, gäbe es derzeit noch keine konkreten Pläne hierzu, sondern nur erste Gedanken. So sei grundsätzlich vorstellbar, dass ein ausführlicheres Beschäftigtendatenschutzgesetz in einem solchen zweiten Paket enthalten sein wird.

Fazit

Die bisherigen Überlegungen im Bundesministerium des Inneren und Aussagen anderer Ressorts zeigen, dass es äußert wichtig ist, das Gesetzgebungsverfahren kritisch zu begleiten. Aus diesem Grund haben Digitalcourage und die Deutsche Vereinigung für Datenschutz ein Positionspapier zur Ausgestaltung der Europäischen Datenschutzgrundverordnung erstellt. Mit diesem treten sie insbesondere mit dem Bundesministerium für Inneres in den Dialog.

Digitalcourage & Deutsche Vereinigung für Datenschutz (DVD)

Position zur Ausgestaltung der Europäischen Datenschutzgrundverordnung

Einführung

Ab 25. Mai 2018 wird mit dem Wirksamwerden der am 25. Mai 2016 in Kraft getretenen Europäischen Datenschutz-Grundverordnung (DSGVO) das bisher geltende nationale Datenschutzrecht weitgehend unwirksam. Sie wird den Datenschutz für die Verarbeitung persönlicher Daten in allen Ländern der EU unmittelbar und weitgehend einheitlich regeln. Die Verordnung enthält zahlreiche Konkretisierungsklauseln, die Mitgliedsländer teilweise nutzen müssen, teilweise nutzen können, um ergänzende nationale Datenschutzgesetze zu verabschieden. Unter diesen Klauseln können elementare Fragen des Datenschutzes beantwortet werden, zum Beispiel zum Beschäftigtendatenschutz, zur Verarbeitung von Gesundheitsdaten, zur Datennutzung für Forschungszwecke, zum Kreditscoring, zur Beschränkung der Rechte von Betroffenen oder zur Bindung der Datenverarbeitung an bestimmte Zwecke.

Digitalcourage und DVD plädieren dafür, dass Deutschland bei der Ausgestaltung der Europäischen Datenschutz-Grundverordnung eine Vorbildrolle für den Schutz von persönlichen Daten einnimmt. Die Konkretisierungsklauseln müssen im Sinne der zentralen Grundsätze der Datenschutzgrundverordnung in Artikel 5 genutzt werden.

Die deutsche Konkretisierung, Ausgestaltung und Interpretation der Europäischen Datenschutz-Grundverordnung muss sich an den ersten beiden Artikeln des Grundgesetzes orientieren, aus denen das Allgemeine Persönlichkeitsrecht, das Recht auf Privatsphäre, das Recht auf informationelle Selbstbestimmung sowie das Recht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme abgeleitet werden.

Auf europäischer Ebene geben die Artikel sieben und acht der EU-Grundrechtecharta die Richtung für die Ausgestaltung der Europäischen Datenschutzgrundverordnung vor: das Recht auf Schutz personenbezogener Daten und das Recht auf Achtung des Privatlebens und der Kommunikation.

Das bestehende deutsche Datenschutzniveau darf nicht abgeschwächt werden. Digitalcourage und DVD fordern deshalb Bundes- und Landesgesetzgeber auf, die nationalen Spielräume konkret wie folgt zu nutzen:

Forderungen zur Nutzung der Konkretisierungsklauseln

– Scoring, automatisierte Einzelfallentscheidungen und Profilbildung: Artikel 22 der Grundverordnung schützt Betroffene vor automatisierten Einzelfallentscheidungen inklusive Scoring und Profiling, wenn diese Datenverarbeitung rechtliche Wirkung entfaltet oder die Betroffenen durch die Verarbeitung ähnlich beeinträchtigt werden. Eine Handlungsoption ermöglicht den Mitgliedstaaten weitere Ausnahmen vom grundsätzlichen Verbot in Absatz 1 zu regeln. Digitalcourage und DVD fordern: Keine weiteren nationalen Ausnahmen für das Verbot von automatisierten Einzelfallentscheidungen sowie Erhalt des bestehenden deutschen Datenschutzniveaus bei Auskunfteien und Scoring. (siehe Position des Verbraucherzentrale Bundesverband e.V.; betrifft: § 28a BDSG, § 28b BDSG, § 34 (Abs. 2-5 u. 8) BDSG sowie § 35 (Abs. 2) BDSG)

– Betroffenenrechte: Kapitel III der Verordnung gibt Betroffenen unter anderem das Recht auf Löschung von Daten (Artikel 17), das Recht auf Auskunft (Artikel 15) und das Recht auf Datenübertragbarkeit (Artikel 20). Nach Artikel 23 der Verordnung können Mitgliedsländer diese Rechte unter bestimmten Bedingungen einschränken. Digitalcourage und DVD fordern: Keine Ausnahmen und Einschränkungen von Betroffenenrechten über das bisher in Deutschland bestehende Maß hinaus. Die Grundverordnung verlangt bei Einschränkungen von Betroffenenrechten, etwa auf Grund der nationalen oder öffentlichen Sicherheit oder auf Grund von Kontroll-, Überwachungs- und Ordnungsfunktionen, die Achtung des Wesensgehaltes der Grundrechte und Grundfreiheiten einer demokratischen Gesellschaft.

– Pflicht zum Hinweisen auf Betroffenenrechte: Betroffene können ihre Rechte nur dann nutzen, wenn sie davon Kenntnis haben. Weil sich die Komplexität von Datenverarbeitung von Betroffenen ohne deutliche, wiederholte und verständliche Hinweise durch Verarbeiter nicht mit hinreichender Sicherheit überschauen lässt, wie es das Bundesverfassungsgericht verlangt, fordern Digitalcourage und DVD die Hinweispflichten auf Betroffenenrechte zu erweitern. (Konkretisierungsklausel für Aufgaben im öffentlichen Interesse: Artikel 6 Absatz 2, Sätze 4 und 5)

– Informationspflichten: Mitgliedstaaten können nach Artikel 14 Absatz 5 der Verordnung Ausnahmen von den Informationspflichten regeln. Digitalcourage und DVD fordern, abgesehen von der Sondersituation bei Berufsgeheimnisträgern, keine Ausnahmen von den Informationspflichten vorzusehen.

– Datenschutz bei Berufsgeheimnisträgern: Artikel 9 verbietet, unter weit formulierten Ausnahmen, die Verarbeitung von besonders sensiblen personenbezogenen Daten. Darunter fallen „Daten, aus denen die rassische und ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen oder die Gewerkschaftszugehörigkeit hervorgehen", sowie genetische und biometrische Daten und

Gesundheitsdaten. Berufsgeheimnisträger, wie etwa Ärtzt.innen oder Anwält.innen dürfen diese Daten verarbeiten. Nach Artikel 90 der Verordnung kann in nationaler Gesetzgebung das Recht auf Schutz der personenbezogenen Daten mit einer Pflicht zur Wahrung des Berufsgeheimnisses in Einklang gebracht werden. Der Datenschutz bei Berufsgeheimnisträgern muss auf bisherigem Niveau beibehalten und, wo nötig, ausgebaut werden. Dazu gehört insbesondere, dass IT-Dienstleister von Berufsgeheimnisträgern sowie Forschende, die mit diesen sensitiven Daten wissenschaftlich arbeiten, vom Privileg und von der Pflicht des Berufsgeheimnisses mit erfasst werden.

– **Beschäftigtendatenschutz:** Die Grundverordnung (Artikel 88) stellt jedem Mitgliedsland die Schaffung eines Beschäftigtendatenschutzgesetzes frei. Digitalcourage und DVD fordern dringend einen starken und umfangreichen Beschäftigtendatenschutz, was angesichts der technischen Entwicklung im Arbeitsleben nur mit einem eigenständigen Beschäftigtendatenschutzgesetz möglich ist. Insbesondere müssen reguliert werden: Überwachung am Arbeitsplatz (Artikel 88 Absatz 2), die Einwilligung im Beschäftigtenkontext, Transparenz der Datenverarbeitung und wirksame Sanktionen der Rechtsdurchsetzung (Artikel 84). Für die Konkretisierung der Regelungen zum Beschäftigtendatenschutz in Kollektivvereinbarungen bedarf es Verfahrensregelungen, die es Arbeitgeber.innen und Arbeitnehmer.innen unter aufsichtsbehördlicher Kontrolle ermöglichen, die Datenverarbeitung rund um den Arbeitsplatz so überwachungsfrei wie möglich zu regeln.

– **Zweckänderung:** Artikel 6 der Verordnung erlaubt Mitgliedsstaaten unter anderem, Anforderungen für die Verarbeitung von Daten im öffentlichen Interesse genauer zu regulieren. Digitalcourage und DVD plädieren dafür, die Regulierungsmöglichkeiten in Artikel 6 im Sinne einer Stärkung des Datenschutzes, also restriktiv, wahrzunehmen. Beispielsweise ist eine nationale Erweiterung von Weiterverarbeitungsmöglichkeiten von persönlichen Daten auszuschließen, etwa bei der Videoüberwachung öffentlich zugänglicher Räume durch Private.*

– **Verarbeitung von genetischen, biometrischen oder Gesundheitsdaten:** Artikel 9 der Verordnung gibt Mitgliedstaaten die Möglichkeit, die Verarbeitung solcher Daten weiter zu beschränken oder auch zu erweitern. Digitalcourage und DVD fordern, dass die Verarbeitung von genetischen, biometrischen oder Gesundheitsdaten auf das unbedingt Notwendige beschränkt wird.

– **Stärkung der Befugnisse der Aufsichtsbehörden:** Der Europäische Gerichtshof hat darauf hingewiesen, dass den Datenschutzaufsichtsbehörden gegen sie verpflichtende Normen Klagebefugnisse zustehen müssen; hierfür bedarf es einer Regelung ohne prozessuale Beschränkungen. Die Aufsichtsbehörden müssen die Möglichkeit haben, effektive Sanktionen auch gegenüber Behörden zu verhängen. Dazu gehört auch, dass diese, anders als bisher, so ausgestattet werden, dass sie ihre Aufgabe des digitalen Grundrechtsschutz effektiv wahrnehmen können. Die Höhe der Geldbußen gegen Behörden muss ein wirksames Mittel zum Schutz der Privatsphäre der Bürgerinnen und Bürger sein.*

– **Betrieblichen Datenschutzbeauftragte:** Die Verpflichtungen für Firmen in der Verordnung, eine oder einen Datenschutzbeauftragten zu bestellen, sind restriktiver als derzeit im Bundesdatenschutzgesetz geregelt. Artikel 35 Absatz 4 erlaubt Mitgliedsstaaten die Beibehaltung der gegenwärtigen nationalen Regelungen. Digitalcourage und DVD fordern, dass die Verpflichtung zur Bestellung betrieblicher Datenschutzbeauftragter nach § 4f Abs. 1 des Bundesdatenschutzgesetzes inhaltlich beibehalten wird. Ohne eine solche Regelung würde das deutsche Datenschutz-Niveau erheblich gesenkt werden.*

– **Regulierung von Beobachtungsmaßnahmen:** Personenbezogene Daten, die durch Beobachtungen wie Videoüberwachung, Smart Meter, Smart Home, RFID oder vernetzten Straßenverkehr verarbeitet werden, sind durch die Europäische Datenschutzgrundverordnung nicht wie bisher im deutschen Datenschutzrecht geschützt. Teilweise erfassen diese Beobachtungen Daten, aus denen ohne Aufwand hochsensible Informationen, etwa über die Gesundheit oder die politische Einstellung, abgeleitet werden können. Darum müssen betroffene Personen besonders durch konkretisierende Festlegungen geschützt werden. Das umfasst: Regelungen zur Transparenz, Datenminimierung, Datensicherheit, Opt-in-Optionen, Ausschluss der Datenweitergabe etc.

– **Vermutungswirkung für Ko-Regulierungen:** Ko-Regulierungen gemäß Artikel 38 wie Gütesiegel, Zertifikate oder Verhaltenskodizes können helfen, den Schutz von personenbezogenen und personenbeziehbaren Daten zu erhöhen. In Ko-Regulierungen können Prinzipien wie Privacy by Design und Privacy by Default, Souveränität über Geräte und deren Datenverarbeitung oder Privacy by Default branchenspezifisch und technisch konkret im Handeln von Unternehmen verankert werden. Besonders weil sich datenverarbeitende Technologien und Anwendung schneller entwickeln als Gesetzgeber Regulierungen schaffen können, sind Ko-Regulierungen wichtige Instrumente für einen wirksamen Datenschutz. Voraussetzung dafür ist, dass eine wirksame behördliche Kontrolle der Ko-Regulierungen stattfindet, dass größtmögliche Transparenz realisiert wird und Betroffenen-Vertretungen bei Ausarbeitung und Anwendung der Ko-Regulierungen effektiv eingebunden werden.

– **Folgenabschätzung und Vorabkonsultation:** Digitalcourage und DVD fordern eine gesetzliche Ausgestaltung der Folgenabschätzungen. Mitgliedstaaten können nach Artikel 35 Absatz 4 bei Datenverarbeitungen auf Basis von Gesetzen der Mitgliedstaaten laut Artikel 6 Absatz 1 gesetzlich regeln, dass eine Folgenabschätzung durchzuführen ist. Außerdem sollten bei der Verarbeitung zur Erfüllung einer im öffentlichen Interesse liegenden Aufgabe nach Artikel 36 Absatz 5 Verarbeiter angehalten sein, mit der verantwortlichen Aufsichtsbehörde eine Vorabkonsultation durchzuführen und eine Genehmigung einzuholen.

* Siehe Position der Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder unter: http://www.bfdi.bund.de/SharedDocs/Publikationen/Entschliessungssammlung/DSBundLaender/91DSK_EntschliessungDSStaerken.pdf?__blob=publicationFile&v=5

BigBrotherAwards 2016

Ein Rückblick von Frans Jozef Valenta

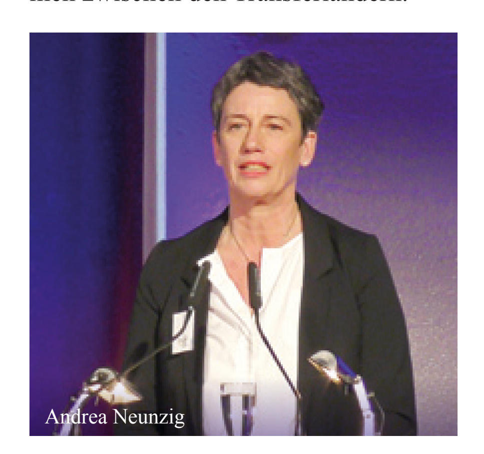

Sabine Leutheusser-Schnarrenberger


Sönke Hilbrans | Peter Wedde

Die Eröffnungsrede bei den BigBrotherAwards in Bielefeld hielt Sabine Leutheusser-Schnarrenberger. Sie würdigte die Verdienste von Digitalcourage bei der Verteidigung des Rechts auf informationelle Selbstbestimmung und zum Schutz der Privatsphäre. „Angst darf nicht als Anlass dienen, die Eingriffsbefugnisse zur massenhaften Überwachung der Bürger immer weiter auszudehnen“. Am Beispiel des in der EU gescheiterten Urheberrechtsabkommens ACTA machte sie deutlich, dass sich beharrlicher Protest lohnt.

Padeluun

In der Kategorie Verbraucherschutz hielt Padeluun die Laudatio wegen der Rabattgewährung bei der Übermittlung von Fitness-Daten an den Versicherungskonzern Generali. Nach dem Muster von Payback geraten die Versicherungskunden in ein Kundenbindungs- und Gängelungssystem. Mit den Punkten der Generali Versicherung können Versicherte sich nicht günstiger versichern, denn für die Punkte bekommen sie Rabatte in Läden, die sich dem Generali-Programm angeschlossen haben – allerdings nur, wenn sie besonders gesunde Produkte kaufen. Und diese müssen sie ausschließlich in bestimmten – aber wenigen – Markengeschäften erwerben. Die intimen Fitnessdaten werden im Rahmen des „Vitality-Programms“ an ein südafrikanisches Finanzunternehmen übermittelt – ohne ein existierendes Datenschutzabkommen zwischen den Transferländern.


Andrea Neunzig

Die von Martin Haase und Kai Biermann verfasste Laudatio in der Kategorie Neusprech mit dem Begriff „Datenreichtum“ wurde von Andrea Neunzig vorgetragen.

Die Laudatoren für Kampagnenplattform change.org in der Kategorie Wirtschaft waren Peter Wedde und Sönke Hilbrans. change.org bekam den BigBrotherAward, „weil sie die personenbezogenen Daten der Menschen, die Petitionen unterzeichnet haben, in vielfältiger und nicht transparenter Art und Weise für eigene Geschäftszwecke verwendet“. Der Organisation wird vorgeworfen, E-Mail-Handel zu betreiben und mit den gewonnenen sensiblen Daten Nutzerprofile zu erstellen, die geeignet wären, Meinungsbildungsprozesse gezielt zu beeinflussen. Abgesehen von der in Deutschland und Europa datenschutzrechtlichen Unzulässigkeit der Verarbeitung und Nutzung dieser personenbezogenen Daten wie insbesondere der Informationen zu politischen Meinungen, wird zur Datenübermittlung immer noch das vom Europäischen Gerichtshof verworfene Safe-Harbor-Abkommen zugrunde gelegt. Der Geschäftsführer von change.org nahm die „Auszeichnung“ widerwillig entgegen, um die Gelegenheit zu einer Stellungnahme zu erhalten.


Andreas Liebold
Gregor Hackmack
Jeannette Gusko


Rena Tangens

Rena Tangens hielt die Laudatio in der Kategorie Technik anlässlich der datenschutzrechtlich verwerflichen Einführung der kontaktlosen Chipkarte „(((eTicket“ durch die Berliner Verkehrsbetriebe (BVG). Der Berliner Fahrgastverband IGEB fand heraus, dass mit Hilfe der kontaktlosen NFC-Technik Trackingdaten erhoben wurden. Es wurde die Frage gestellt, warum überhaupt Streckendaten erfasst werden müssen und erfolgreiche alternative Beispiele mit kostenlosem Bus- und Bahnverkehr genannt.


Frank Rosengart

Die IBM Deutschland GmbH erhielt die Auszeichnung in der Kategorie Arbeitswelt. Frank Rosengart erläuterte in seiner Laudatio die Auswertung von Daten aus dem firmeneigenen sozialen Netzwerk mit der Software „Social Dashboard“. So könne ein Arbeitgeber neue Einblicke erhalten, wer welchen sozialen Status und Vernetzungsgrad unter seinen Kollegen hat. Alles wird zum Wettbewerb, zur „Challenge“.


Andreas Liebold | Rena Tangens

Rena Tangens nannte in einem Interview die Erfolge seit der Preisverleihung 2015. Dazu gehörte auch die Aktivität auf dem Evangelischen Kirchentag (DANA 3/2015, S. 140) und der Start zu einer neuen Verfassungsklage gegen die Vorratsdatenspeicherung.


Andreas Liebold

Leena Simon

Leena Simon zählte eine Reihe von tadelnden Erwähnungen auf: das sogenannte „Prostituiertenschutzgesetz“, die Google Impact Challenge, bei der der Konzern die Zivilgesellschaft als Datenquelle entdeckt hat, und das Cashless Festival, bei dem Festival-Besucher mit einem RFID-Armband zur Konsum-Kontrolle ausgestattet wurden. Eine lobende Erwähnung gab es für Jan Philipp Albrecht & Team für die Arbeit an der EU-Datenschutzgrundverordnung.



Rolf Gössner

Der Inlandsgeheimdienst „Verfassungsschutz“ ist bisher erstaunlicherweise in den 16 Jahren seit Bestehen des BigBrotherAward nie mit einem Preis bedacht worden. Für eine 65-jährige Geschichte war deshalb ein Lifetime-Award fällig. Rolf Gössner erinnerte in seiner Laudatio an „Skandale und Machtmissbrauch, Datenschutz- und Bürgerrechtsverletzungen – selbstverständlich immer im Namen von Sicherheit und Freiheit, Verfassung und Demokratie“. Gössner erklärte weiter: „Hinter dem irreführenden Tarnnamen ‚Verfassungsschutz‘ steckt ein ideologisch geprägter Regierungsgeheimdienst mit geheimen Mitteln und Methoden wie V-Leuten, verdeckten Ermittlern, Lockspitzeln, Lausch- und Spähangriffen und der Lizenz zur Infiltration, Täuschung und Desinformation – Mittel und Methoden, die gemeinhin als ‚anrüchig‘ gelten und die sich rechtsstaatlicher Kontrolle weitgehend entziehen“.

Datenschutznachrichten

Datenschutznachrichten aus Deutschland

Bund

Kartellamt ermittelt gegen Facebook

Das Bundeskartellamt prüft seit dem 02.03.2016, ob die Nutzungsbedingungen von Facebook rechtswidrig sind. Die Nutzenden von Facebook könnten nur schwer nachvollziehen, welchen Umfang ihre Einwilligung zur Erhebung und Nutzung ihrer Daten hat. Das soziale Netzwerk steht unter dem Verdacht, seine Marktmacht auszunutzen. Es bestünden „erhebliche Zweifel“ an der Zulässigkeit dieser Vorgehensweise – insbesondere nach deutschem Datenschutzrecht. Im Zentrum der Nachforschungen stehen die komplizierten Nutzungsbedingungen, mit denen die Nutzenden umfassend akzeptieren müssen, dass Facebook umfangreich persönliche Daten erhebt und verwendet, ohne dass diese dies hinreichend nachvollziehen können.

Weil es „Anhaltspunkte“ gäbe, dass Facebook auf dem Markt für soziale Netzwerke marktbeherrschend sei, könnte ein solcher Verstoß auch kartellrechtlich missbräuchlich sein. Facebooks Daten ermöglichten, so Kartellamtspräsident Andreas Mundt, durch die Bildung von Nutzungsprofilen Werbekunden ein zielgenaues Werben: „Marktbeherrschende Unternehmen unterliegen besonderen Pflichten“. Das Verfahren richtet sich gegen den Konzern Facebook in den USA, gegen die irische Tochter des Unternehmens sowie gegen Facebook Germany in Hamburg. Facebook ist das größte soziale Netzwerk der Welt. Weltweit nutzen es täglich mehr als eine Milliarde Menschen. 1,6 Mrd. Menschen schauen mindestens einmal im Monat vorbei. In Deutschland sind etwa 28 Mio. Menschen Mitglied, die meisten zwischen 18 und 44 Jahren – eine für die Werbewirtschaft höchst attraktive Gruppe. Mundt: „Für werbefinanzierte Internetdienste wie Facebook haben die Nutzerdaten eine herausragende Bedeutung.“ Bei Internetdiensten gebe es einen Trend zur Monopolisierung. Doch tut sich seine Behörde schwer bei grenzüberschreitenden Unternehmen. Das Kartellamt könnte, sollte sich der Verdacht erhärten, eine Änderung der beanstandeten Klauseln verlangen.

Facebook reagierte gelassen: „Wir sind überzeugt, dass wir das Recht befolgen, und werden aktiv mit dem Bundeskartellamt zusammenarbeiten, um dessen Fragen zu beantworten“. Diverse deutsche Datenschützer und Verbraucherorganisationen werfen Facebook schon seit einiger Zeit vor, zu viele Daten zu erheben und dies nicht transparent genug zu tun. Das Kartellamt betreibt das Verfahren in engem Kontakt unter anderem mit Datenschutzbeauftragten, Verbraucherschutzverbänden und der EU-Kommission. Klaus Müller, Vorstand der Verbraucherzentrale Bundesverband (vzbv), erklärte: „Verbraucher haben zu Facebook keine adäquate Alternative, ihre Nutzungsdaten können sie nicht ohne Weiteres auf andere Portale übertragen.“ Diese „Zwangslage“ sei ähnlich kritisch zu sehen wie „unfaire Monopolpreise in der analogen Welt“ (Bauchmüller/Martin-Jung, Kartellamt geht gegen Facebook vor, SZ 03.03.2016, 1; Kartellamt ermittelt wegen des Verdachts auf Marktmissbrauch, www.zeit.de 02.03.2016).

Bund

Flugtauglichkeitsprüfung unter Aufhebung des Patientengeheimnisses

Nach Auffassung von Bundesverkehrsminister Alexander Dobrindt (CSU) soll es in Zukunft schwerer werden für psychisch labile oder gesundheitlich angeschlagene PilotInnen, sich dem Kontrollsystem der Flugaufsichtsbehörden zu entziehen. Wegen der in Deutschland für VerkehrspilotInnen geltenden Regelungen, die im Hinblick auf ärztliche Schweigepflicht und Datenschutz europaweit als die strengsten gelten, liegen beim Luftfahrtbundesamt (LBA) die Gesundheitsakten der PilotInnen nur in pseudonymisierter Form, also ohne namentliche Nennung, vor. Nur nach einem aufwändigen Verfahren könnten Untersuchungsergebnisse einem individuellen Piloten zugeordnet werden. Den Gesundheits-Check-up machen niedergelassene Fliegerärzte und melden dem LBA lediglich, dass der Flugzeugführer „fit to fly“ ist.

- Der Germanwings-Absturz

Dies mag dazu beigetragen haben, dass die Depression des Germanwing-Piloten Andreas Lubitz, der am 24.03.2015 149 Menschen mit in den Tod riss, den verantwortlichen Stellen unbekannt blieb (vgl. DANA 2/2015, 82 ff.), obwohl er in den letzten Monaten seines Lebens von Mediziner zu Mediziner lief, Psychopharmaka verschrieben bekam und sich in Psychotherapie begab. Weder bei der Airline noch beim Luftfahrtbundesamt (LBA) bekam man mit, wie sich sein psychischer Zustand verschlimmerte – bis er seinen Wunsch nach Selbstmord in einem kontrollierten Absturz in den französischen Alpen in die Realität umsetzte.

Selbst wenn einer der von Lubitz aufgesuchten Mediziner, ob Fliegerarzt oder niedergelassener Arzt, sich Sorgen um dessen labile Psyche gemacht hätte, so hätte er vom LBA nicht erfahren können, dass der 26-jährige Co-Pilot bereits während seiner Ausbildung an einer schweren suizidalen Erkrankung gelitten hatte. Diese Information hätte er sich, umständlich, von dem behandelnden Fliegerarzt im flugmedizini-

schen Zentrum der Lufthansa besorgen müssen. Dabei wäre diese entscheidend gewesen für seine flugmedizinische Beurteilung. Denn tritt eine Depression erneut auf, so bedeutet das in der Regel den Entzug der Lizenz.

In einem umfangreichen Bericht der französischen Behörde für die Untersuchung ziviler Flugunfälle (BEA) kommt diese zu dem Ergebnis: „Der Prozess der medizinischen Begutachtung des Copiloten war konform mit den Regeln, die zu der Zeit in Deutschland galten." In der Präsentation des Berichts drängte aber BEA-Direktor Rémi Jouty darauf, diese Regeln in Deutschland und Europa zu ändern. Die BEA verlangt u. a., die ärztliche Schweigepflicht zu lockern und klarer und konkreter als bisher im Interesse der „öffentlichen Sicherheit" Ausnahmen vorzusehen. Er erwähnte lobend, dass in Israel, Kanada und Norwegen sogar eine Pflicht zur Information des Arbeitgebers besteht. Weiterhin empfiehlt der Bericht, PilotInnen weitaus häufiger „psychologisch und psychiatrisch" auf die Flugfähigkeit zu testen. Zudem befürwortet er, nach britischem Vorbild und unter ärztlicher Aufsicht PilotInnen unter dem Einfluss von Psychopharmaka fliegen zu lassen, weil sie ansonsten, wie Andreas Lubitz, ihre Krankheit verheimlichen könnten. Schließlich schlägt die BEA bessere Verdienstausfall-Versicherungen für flugunfähige PilotInnen im Interesse von deren finanzieller Absicherung vor.

Allein 124 Seiten ist die Zusammenfassung des BEA-Reports lang. Die gesamte Untersuchung ist mit Dokumenten 6000 Seiten stark. Darin wird nacherzählt, dass Andreas Lubitz insgesamt 41 Ärzte konsultiert hatte und dies schon August 2008, noch während seiner Ausbildung bei der Lufthansa. Im Dezember 2014 hatten „verschiedene Ärzte" festgestellt, dass für die häufigen Seh- und Schlafstörungen ihres Patienten „kein organischer Grund" vorlag. Am 17.02.2015 hatte Lubitz wegen seines psychischen Leidens zwei Ärzte aufgesucht. Ein privater Arzt schrieb ihn für acht Tage krank. Ein weiterer privater Arzt stellte ihm ein Rezept für das Schlafmittel Zopiclon aus. Alles dies verschwieg der Copilot seinem Arbeitgeber, ebenso eine Überweisung für eine stationäre psychiatrische Behandlung am 10.03.2015 und ein Arbeitsunfähigkeitsattest für 19 Tage vom 12.03.2015. Die bestehende Pflicht zur Selbstanzeige funktionierte nicht.

Die Pilotengewerkschaft Cockpit begrüßte die Empfehlungen der BEA im Grundsatz. Hinsichtlich der Entbindung von der ärztlichen Schweigepflicht jedoch gab man sich vorsichtig. Es müssten weiterhin strenge Kriterien angelegt werden, damit die Privatsphäre geschützt bleibe. Es sei bereits jetzt grundsätzlich möglich, bei Gefahr im Verzug medizinische Daten weiterzugeben.

- Der Gesetzentwurf

Die bisherige Überprüfungs- und Meldepraxis wurde auch durch die EU-Kommission gerügt und ein Vertragsverletzungsverfahren gegen Deutschland, konkret das Dobrindt-Ministerium, eingeleitet. Auf dessen Initiative hin will die Regierungskoalition nun das Luftverkehrsgesetz ändern und die Pseudonymisierung beenden. Dazu soll „eine elektronische Datenbank über durchgeführte flugmedizinische Untersuchungen und Beurteilungen" beim LBA angelegt werden, damit die Behörde ihre Aufsicht über die flugmedizinischen Zentren „sicherstellt".

Die Datenbank soll sämtliche Untersuchungsberichte bei festgestellter Untauglichkeit enthalten, und zwar personenbezogen und namentlich. Zugriff darauf soll die flugmedizinische Abteilung des LBA haben. Die dortigen MedizinerInnen, die der Schweigepflicht unterliegen, sollen bei Zweifeln an der Tauglichkeit des Piloten eingreifen und die Lizenz zurückziehen können. All dies war bisher praktisch unmöglich. Zusätzlich soll es in Zukunft einen fliegerärztlichen Ausschuss geben, der das LBA bei dem Verdacht einer Gesundheitsstörung bei PilotInnen beraten soll.

Die Koalitionsfraktionen haben einen entsprechenden Gesetzentwurf in den Bundestag eingebracht. Darin begründen die Regierungsparteien, in der Vergangenheit seien Mehrfachuntersuchungen einer Piloten-BewerberIn nicht festgestellt worden und eine Art „Tauglichkeitstourismus" sei entstanden: Erhält eine PilotIn eine ihre Tauglichkeit gefährdende oder gar verneinende Diagnose, geht sie einfach zum nächsten Arzt – bis sie seinen Freischein hat. Nach dem Entwurf müssen Fluggesellschaften bei ihrem Personal künftig vor Dienstbeginn Kontrollen auf Medikamente, Alkohol oder andere psychoaktive Substanzen durchführen, „wenn ein auf Tatsachen begründeter Verdacht vorliegt, dass die Dienstfähigkeit der betreffenden Person wegen der Einnahme dieser Mittel beeinträchtigt oder ausgeschlossen ist". Zusätzlich soll es präventive Zufallskontrollen geben. Diese müssen auch unter ärztlicher Aufsicht durchgeführt werden. Wie die Kontrollen konkret vorgenommen werden, sollen Arbeitgeber und Gewerkschaften in Tarifverträgen oder Betriebsvereinbarungen regeln. Die EU-Aufsichtsbehörde hatte unangekündigte Alkohol- und Drogentests gefordert. Bislang ist Deutschland, so der Entwurf, „das einzige EU-Land", das entsprechende internationale Bestimmungen der Flugmedizin mit zusätzlichen Datenschutzbestimmungen eingeführt hat.

Widerstand gegen das veränderte Luftverkehrsgesetz leisten die PilotInnen. Der Sprecher der Pilotenvereinigung Cockpit, Markus Wahl, bezeichnet die Gesetzesnovelle als kontraproduktiv. Es werde die ärztliche Schweigepflicht aufgehoben, wenn medizinische Daten an das LBA gemeldet werden: „Kollegen mit gesundheitlichen oder psychischen Problemen werden sich aus Angst vor Sanktionen künftig nicht mehr einem Arzt anvertrauen". Es wäre somit die vollkommen falsche Lehre aus der Germanwings-Katastrophe, die flugmedizinischen Regeln zu verschärfen.

Die Taskforce, zusammengesetzt aus Airlines, Behörden und PilotInnen, die das Bundesverkehrsministerium nach dem Absturz in Frankreich eingerichtet hatte, sprach sich für die Abschaffung der Pseudonymisierung aus. Der Vorsitzende der Kommission, Matthias von Randow vom Bundesverband der deutschen Luftverkehrswirtschaft (BDL), sagte bei der Vorstellung eines Zwischenberichts im Sommer 2015, dass durch einen solchen Schritt „die Untersuchungs- und Kontrollpraxis vereinfacht" werde (Traufetter, Ende der Anonymität, www.spiegel.de 22.02.2016; Corneloup, Unangekündigte Pilotenkontrollen sollen ins Luftverkehrsgesetz einfließen, www.airliners.de 22.02.2016; Christina

Berndt, Die Lehren aus der Katastrophe, SZ 14.03.2015, 8).

Bund

vzbv klagt gegen Google wegen Mail-Inhaltskontrolle

Der Verbraucherzentrale Bundesverband (vzbv) hat erneut zwei Klauseln in der Datenschutzerklärung von Google abgemahnt. Es geht um die Erhebung und Verwendung von personenbezogenen Daten. Zwei Nutzungsbedingungen enthielten Formulierungen, die die Rechte der VerbraucherInnen nach Ansicht des vzbv unzulässig einschränken. Der Konzern maßt sich an, automatisiert Inhalte der NutzerInnen, zum Beispiel E-Mails beim Dienst Gmail, zu analysieren, um etwa personalisierte Werbung zu platzieren. Der vzbv hält das für rechtswidrig, weil es an einer wirksamen Einwilligung in diesen intensiven Eingriff fehlt. Viele E-Mails enthalten sehr private und höchstpersönliche Informationen, die durch das Telekommunikationsgeheimnis besonders geschützt sind. Diese stammen nicht immer nur von der NutzerIn, sondern oft auch von Dritten, die E-Mails an die NutzerIn senden. Dazu Klaus Müller: „Es kann nicht sein, dass Google die E-Mails seiner Nutzer ohne spezifische Einwilligung mitliest, um diesen dann maßgeschneiderte Produktinformationen anzuzeigen."

Der vzbv geht davon aus, dass es für die Erhebung und Nutzung personenbezogener Daten zu Werbezwecken immer eine gesonderte Einwilligung geben muss. In einzelnen Klauseln der aktuellen Datenschutzerklärung wird diese Praxis zwar allgemein angekündigt, allerdings ohne die VerbraucherIn um Zustimmung zur konkreten Datenerhebung und Datennutzung zu bitten. Dass die Nutzenden aufgefordert werden, der Datenschutzerklärung von Google insgesamt zuzustimmen, genügt dem vzbv nicht. Der Begriff „Werbung" wird in diesem Zusammenhang nicht näher beschrieben, so dass er theoretisch sogar Anrufe bei der NutzerIn umfasst. Heiko Dünkel, Referent im Team Rechtsdurchsetzung beim vzbv: „Auf welchen Kanälen und für welche Produktgruppen geworben werden soll, ist für den Verbraucher nicht klar erkennbar."

Der vzbv beanstandet zudem eine Klausel, nach der nur für die Weitergabe „sensibler Kategorien" von personenbezogenen Daten eine ausdrückliche Einwilligungserklärung notwendig ist. Eine Unterscheidung zwischen „sensiblen" und anderen personenbezogenen Daten ist nach Ansicht des vzbv mit den deutschen Datenschutzvorschriften nicht vereinbar.

Der vzbv hatte bereits 2012 gegen 25 Klauseln der damaligen Datenschutzerklärung und Nutzungsbedingungen geklagt und im November 2013 vor dem Landgericht Berlin gewonnen. Dagegen ist der Konzern in Berufung gegangen. Dieses Verfahren liegt derzeit beim Kammergericht. Google hat dann im Sommer 2015 seine Datenschutzbestimmungen geändert. Allerdings sind die streitgegenständlichen Klauseln zum Teil immer noch darin zu finden. Auf die Abmahnung durch den vzbv zu den beiden weiteren Klauseln aus der aktuellen Datenschutzerklärung hatte Google bis zum vorgegebenen Termin am 12.02.2016 nicht reagiert, so dass der vzbv nun eine Unterlassungsklage vor dem Landgericht Berlin erhob (vzbv PM v. 26.02.2016, vzbv mahnt Datenschutzerklärung von Google erneut ab; Mossbrucker, Verbraucherschützer klagen gegen Google, SZ 26.02.2016, 22).

Bund

Bundestrojaner ist einsatzbereit

Nach monatelangen Vorbereitungen steht den Ermittlern von Bund und Ländern die umstrittene eigene Software für Online-Durchsuchungen zur Verfügung. Ein Sprecher des Bundesinnenministeriums (BMI) teilte mit, dass die Genehmigung für den sogenannten Bundestrojaner erteilt worden sei. Die technischen Tests und der notwendige rechtliche Vorlauf seien abgeschlossen. Der Bundestrojaner könne jederzeit zum Einsatz kommen. Ursprünglich wollte das Bundeskriminalamt (BKA) ihn im Herbst 2015 einsatzbereit haben.

Bei der Online-Durchsuchung werden Daten auf den Speichermedien von Computern oder Smartphones eines Verdächtigen abgeschöpft. Das Programm dient der Überwachung laufender Gespräche und Chats. Der Ministeriumssprecher erläuterte: „Grundsätzlich ist das eine Fähigkeit an einer Stelle, wo es eine solche Fähigkeit nicht gab." Die Software dient der Quellen-Telekommunikationsüberwachung. Sie soll es den Ermittlern ermöglichen, Kommunikation mitzuverfolgen, bevor sie verschlüsselt ist. Die Freigabe sei „nach umfassenden Tests und einer externen Software-Prüfung" im Herbst 2015 erfolgt. Auch die Landeskriminalämter könnten das Programm nutzen; ihre MitarbeiterInnen müssten aber noch geschult werden.

Beim Bundestrojaner handelt es sich um ein Programm, das – wie ein trojanisches Pferd – auf den Rechner des Verdächtigen gespielt werden und den Ermittlern dann über das Internet die Chance geben soll, die Kommunikation mit dem Gerät mitzuhören oder zu lesen. Einer Vorgängerversion, die Ermittler nicht nur mitlesen ließ, sondern gleich Zugriff auf den ganzen Rechner ermöglichte, setzte das Bundesverfassungsgericht 2008 enge Grenzen, die von der neuen Software beachtet werden sollen. Der Sprecher des Innenministeriums betonte, das Instrument komme nur aufgrund gesetzlicher Voraussetzungen zum Einsatz. Die Bundesdatenschutzbeauftragte Andrea Voßhoff sei beteiligt gewesen.

Der Grünen-Fraktionsvize Konstantin von Notz zeigte sich skeptisch, ob der Trojaner verfassungskonform eingesetzt werden kann: „Das Bundesverfassungsgericht hat klargemacht, dass ein heimlicher Fernzugriff nur unter strengsten Voraussetzungen und bei überragend wichtigen Rechtsgütern zulässig sein kann." Dies ist demnach etwa bei Gefahr für Leib und Leben oder Delikten gegen den Bestand des Staats der Fall. Von Notz forderte unter anderem, dass der dem Programm zugrundeliegende Quellcode offengelegt werden müsse, also der Programmiertext der Software. Ähnlich äußerte sich auch für den Chaos Computer Club (CCC) Falk Garbsch: „Es ist fast unmöglich nachzuweisen, dass ein Programm eine bestimmte Funktion nicht hat." Der CCC hatte 2011 eine ähnliche Software bayerischer Behörden analy-

siert und festgestellt, dass das Programm einen umfassenden Zugriff auf die Speicher der Zielpersonen sowie die Fernsteuerung der Rechner ermöglichte. Der CCC wies zudem darauf hin, dass ein Trojaner immer auch ein Einfallstor für andere Kriminelle ist. Diese könnten sich Schwachstellen in der Software zunutze machen, die Funktionen des Trojaners erweitern und ihre eigenen Programme einschleusen. So könnten sich z. B. ausländische Geheimdienste oder Kriminelle Zugang zu Rechnern von Verdächtigen verschaffen, die von deutschen Behörden überwacht werden (BKA-Software zur Online-Überwachung einsatzbereit, www.focus.de 22.02.2016; BKA setzt nun „Bundestrojaner“ ein, SZ 23.02.2016, 7).

Bund

BND-US-Kooperation läuft wieder

Gemäß Presseberichten haben der deutsche Bundesnachrichtendienst (BND) und der US-Geheimdienst National Security Agency (NSA) die gemeinsame Überwachung des Internets über die Abhörstation in Bad Aibling wieder aufgenommen; wo Parabolspiegel, die sich unter den überdimensionierten Golfbällen verbergen, auf Satelliten ausgerichtet sind. Die Station fängt nach Angaben aus Regierungskreisen vor allem Kommunikation aus dem sogenannten islamischen Krisenbogen ab – Afghanistan, Syrien, dem Irak, Libyen.

Im Mai 2015 war die Lausch-Kooperation nach einem Eklat ausgesetzt worden. Seit 2002 hatten NSA und BND hier zusammengearbeitet. Laut der streng-geheimen Vereinbarung sollte es vor allem um die Suche nach Terroristen und Waffenschiebern gehen. Doch dann kam heraus, dass die NSA den deutschen Freunden Zehntausende Suchbegriffe, sogenannte Selektoren, untergeschoben hatte, die gar nichts mit der Suche nach Kriminellen zu tun hatten. Es ging um ganz gewöhnliche Spionage – auch gegen DiplomatInnen und SpitzenpolitikerInn befreundeter EU-Staaten. Das Kanzleramt war düpiert, der BND wurde angewiesen, künftig für jeden von den Amerikanern übermittelten Suchbegriff eine Begründung zu verlangen. So etwas dürfe sich nicht wiederholen.

Die NSA forderte zu Geduld auf. Immerhin hatten die USA den BND zuletzt mit 4,5 Millionen Suchbegriffen beliefert, die 1,2 Millionen Personen und Institutionen betrafen. Nur für abgehörte Telefonnummern gab es jeweils eine kurze Begründung der NSA, nicht für E-Mail-Adressen, das Gros der Überwachung. Kurzerhand beendeten BND und Kanzleramt deshalb diesen Teil der Kooperation. Die Datenbank der NSA für die Internet-Suchbegriffe wurde abgeschaltet. Prompt machten Alarmmeldungen die Runde: Davon werde sich das deutsch-amerikanische Geheimdienstverhältnis nicht erholen, es gebe schon Überlegungen der USA, künftig lieber stärker mit Polen, Skandinaviern oder Franzosen zu kooperieren. Und, besonders gravierend: Deutschland werde künftig weniger Hinweise auf terroristische Bedrohungen erhalten – und stünde schutzlos da.

Nichts davon ist eingetreten. Bereits seit Monaten liefern die US-Amerikaner nun Stück für Stück die eingeforderten Begründungen, der BND gibt sie in seine Computer ein. Vor allem die Netze in den Krisengebieten sollen das Ziel sein. Die erfassten Datenmengen sind riesig. Gerechnet wird in „Sessions“, die jeweils eine Stunde dauern. Vor der teilweisen Stilllegung wurden in einer Session 23 Millionen Rohdaten erfasst. Auf Bad Aibling, das einen „einzigartigen Zugang“ erlaube, wie die NSA einmal schrieb, will man nicht verzichten.

Bisher spricht nichts dafür, dass die Amerikaner erneut versuchen, den Deutschen etwas unterzujubeln. In keinem einzigen Fall soll der BND in den vergangenen Monaten eine der gelieferten Begründungen der NSA als nicht stichhaltig abgelehnt haben. Das Weiße Haus, so heißt es in Berlin, sei zudem zufrieden, dass bisher die meisten der hässlichen Details über amerikanische Spionageoperationen gegen die europäischen Freunde unter der Decke blieben. Genau deshalb hatte das Kanzleramt verfügt, dass nur ein Sonderermittler, aber nicht der NSA-Untersuchungsausschuss des Bundestages, die Einzelheiten erfahren dürfe. Die Opposition im Bundestag klagt dagegen vor dem Bundesverfassungsgericht.

Inzwischen läuft die Kooperation zwischen deutschen und US-Geheimdiensten wieder reibungslos, nichts werde zurückgehalten, heißt es. Auch bei der Terrorwarnung an Silvester 2015/16 in München spielten die Amerikaner eine Rolle. Die Proteste aus Berlin sind leiser geworden. Inzwischen kam heraus, dass auch der BND befreundete Regierungen von Bad Aibling aus ausspionierte. Der Dienststellenleiter wurde wie andere höhere Chargen der Abteilung Technische Aufklärung inzwischen versetzt. Das Kanzleramt plant, nun den Entwurf eines Gesetzes vorlegen, der politische Spionage gegen europäische Freunde verbietet und dem Bundestag ein Kontroll- und Mitspracherecht bei der Frage einräumt, wer künftig abgehört werden darf (Mascolo, Terrorfahndung im Alpenvorland, SZ 09./10.01.2016, 1).

Bund

BND verweigert Datenschutzprüfung

Die Bundesbeauftragte für den Datenschutz und die Informationsfreiheit (BfDI) Andrea Voßhoff wirft dem Bundesnachrichtendienst (BND) in einem 60-seitigen Bericht zur deutsch-US-amerikanischen Kooperation in der Überwachungsstation Bad Aibling vor, ihrer Behörde die sog. NSA-Selektoren nicht zur Prüfung zu überlassen. Dies sei ein „schwerwiegender Verstoß“ gegen das Bundesdatenschutzgesetz (BDSG). Das BDSG schreibt allen öffentlichen Stellen des Bundes vor, die Behörde der BfDI zu unterstützen. Gemäß dem Bericht unterliegen alle Selektoren, die über deutsche Systeme laufen, dem deutschen Recht und damit der BfDI-Kontrolle. Der BND hatte über Jahre hinweg für den US-Geheimdienst NSA Millionen Suchbegriffe, die sog. Selektoren, in seine eigenen Systeme eingespeist. Gemäß der BfDI hätten diese Selektoren niemals verwendet werden dürfen („Schwerwiegender Verstoß“, Der Spiegel 16/2016, 23).

Bund

Stasi-Unterlagen-Verwaltung soll reformiert werden

Die Expertenkommission zur Reform der Stasi-Unterlagen-Behörde legte dem Kulturausschuss des Bundestags einen Vorschlag vor, wonach aus dem Bundesbeauftragten für die Stasi-Unterlagen eine Art Opferbeauftragter nach dem Vorbild des Patientenbeauftragten werden soll. Das vom früheren Ministerpräsidenten Sachsen-Anhalts, Wolfgang Böhmer (CDU), geführte Gremium will mehrere „Bausteine“ für eine Reform präsentieren. Die Zuständigkeit für die Stasi-Akten soll das Bundesarchiv erhalten. Die Akten sollen jedoch „nutzernah“ bleiben; d. h. die Akteneinsicht soll nicht eingeschränkt werden. Die Forschungsabteilung des Bundesbeauftragten soll eigenständig werden. Die SPD-Fraktion drängt auf eine rasche Umsetzung der Reform, die im Grundsatz im schwarz-roten Koalitionsvertrag vereinbart ist. Sie will Roland Jahn erst für eine zweite Amtszeit wiederwählen, wenn Einigkeit über die Auflösung der einstigen Gauck- bzw. Birthler-Behörde besteht. So lange soll Jahn das Amt kommissarisch führen. Jahn habe Bereitschaft signalisiert, den umgewandelten Posten zu übernehmen (Ende der Jahn-Behörde, Der Spiegel 10/2016, 29).

Bayern

VKB nutzt „künstliche Intelligenz“ zur Sachbearbeitung

Die Versicherungskammer Bayern (VKB) nutzt den IBM-Supercomputer Watson in Kooperation mit der Hochschule für angewandte Wissenschaften in München, um die Tausende Schreiben, die KundInnen zusenden, zu analysieren. Die Software soll, so VKB-Managerin Isabella Martorell Naßl, „Unmutsäußerungen in Kundenschreiben erkennen und in verschiedene Kategorien sortieren“. Ergebnis soll eine passgenaue Antwort sein mit einer Lösung des benannten Problems und kein vertröstendes Standardschreiben. Das Münchener Versicherungsunternehmen erhält jährlich mehr als sieben Millionen Kundenbriefe und Mails. Schon bisher werden sie per Computer analysiert, der die Post nach Schlagworten untersucht, ohne aber den Zusammenhang der Wörter zu erkennen. Angestellte arbeiten manuell nach, um die Schreiben an den richtigen Ansprechpartner zu leiten, der sie dann beantwortet.

Versicherungsangestellte und SprachwissenschaftlerInnen haben Watson u. a. Unmutsäußerungen beigebracht. Das Programm führte dann selbsttätig Analysen durch. Mit dem Ergebnis starteten die Trainer eine neue Runde mit Instruktionen. Inzwischen soll Watson sogar Ironie erkennen können. „Wenn ein Kunde schreibt, ‚vielen Dank für die schnelle Schadenbearbeitung‘, und sich im nächsten Satz beschwert, dann erkennt das Programm das und reagiert entsprechend.“ Watson ordnet die Sätze in den Schreiben in drei Kategorien ein: Auslöser, Unmutsäußerung und Forderung. Auslöser: Niemand hat sich gemeldet. Unmutsäußerung: Die KundIn stellt fest, dass sie keine Reaktion erhalten hat, schreibt: „Ich bin sauer.“ Die Forderung: „Ich bitte Sie nochmals, meinen Sachverhalt zu prüfen und sich mit mir in Verbindung zu setzen.“

Beim Test der VKB, wie gut sich Watson im Vergleich zu Menschen schlägt, die Unterlagen von Hand sortieren, so Naßl, habe die Maschine „sehr überzeugend“ gewonnen. Im nächsten Schritt will die VKB Watson nun im Alltag nutzen. Arbeitsplätze soll das nicht kosten, nur Anpassungen werde es geben. Das Programm analysiert Sprache und reagiert entsprechend. Der Name des Computers bezieht sich auf Thomas Watson, den ersten IBM-Chef. 2011 machte Watson Schlagzeilen, als der Computer die US-Quizshow „Jeopardy“ gewann. Inzwischen ist sein Programm sehr viel weiter entwickelt und wird im Gesundheitswesen, im Einzelhandel, bei der Analyse sozialer Netze und in vielen anderen Wirtschaftsbereichen eingesetzt, darunter Banken und Versicherungen. Die Unternehmen erhoffen sich eine zielgenauere Kundenansprache und auch Kostensenkungen.

Bayerische Besonderheiten, so Naßl, habe das Programm inzwischen auch drauf: „Mit der doppelten Verneinung hat Watson überhaupt keine Probleme“ (Fromme, Ärger an Watson, SZ 09.12.2015, 17).

Bayern

Holtzbrinck plant vollautomatisierte Krankenversicherung nach US-Vorbild

In den USA ist eine vollständig digitalisierte Krankenversicherung mit dem Namen „Oscar“ am Markt, bei der alles, von der Antragstellung über die Arztwahl bis hin zur Patientensteuerung, über eine Smartphone-App erledigt wird. Google hat im September 2015 33 Millionen Dollar bei Oscar investiert. Oscar wird als mögliches Zukunftsmodell weltweit von Krankenkassen und privaten Versicherern aufmerksam verfolgt. Ein Werbevideo beschreibt, wie das System funktioniert: „Hi, we‘re Oscar“. Kundin Joanna hat ein Problem und teilt dies über die App mit: „Ich habe Ausschlag“. Die App antwortet sofort – kostenfrei: „Soll unser diensthabender Arzt anrufen?“ Wenn Joanna zu einem Hautarzt möchte, dann kostet das 100 Dollar (92 Euro) Zuzahlung. Für eine Hausarzt-Konsultation sind nur 60 Dollar fällig. Joanna entscheidet sich für den Hausarzt. Die App schlägt eine Reihe von Medizinern in der Nähe vor und kann die Terminvereinbarung übernehmen. Joanna möchte aber jetzt doch erst den diensthabenden Arzt telefonisch konsultieren und lädt vor dem Gespräch ein Foto ihres Ausschlags hoch.

Der deutsche Investor Dieter von Holtzbrinck plant, in Deutschland mit einem digitalen privaten Krankenversicherer nach dem Vorbild Oscar in den Markt zu gehen. Das Investment wird im zweistelligen Millionenbereich liegen. Im ersten Quartal 2017 soll die Gesellschaft in München an den Start gehen. Der neue Versicherer will sich auf die Kranken-Vollversicherung und die Pflegeversicherung konzentrieren, nicht so sehr auf die Zusatzpolicen für Zahnersatz oder Einbettzimmer im Krankenhaus. Der Unternehmensberater Roman Rittweger leitet den Aufbau und soll

Vorstand werden. Rittweger habe mit der erfolgreichen Gründung der Firma Almeda gezeigt, dass er das Geschäft versteht. Almeda ist Gesundheitsdienstleister für Versicherer, Kassen und andere Firmen.

Bis zum Markteintritt haben die Gründer noch viele Hürden zu nehmen. Sie müssen die Finanzaufsicht Bafin davon überzeugen, dass die künftigen Vorstände geeignet sind und die Finanzplanung solide ist. Angesichts der niedrigen Zinsen ist es nicht einfach, das Unternehmen stabil aufzustellen. Anders als in den USA muss ein privater Krankenversicherer in Deutschland Alterungsrückstellungen aufbauen, damit die Beiträge im Alter – wenn die Gesundheitskosten höher sind – nicht astronomische Höhen erreichen. Wegen der niedrigen Zinsen dürfte das gerade am Anfang nicht einfach sein und viel von den Beiträgen kosten. Die Gründer glauben, dass sie trotzdem wettbewerbsfähig sein werden. Die Digitalisierung sorge für niedrigen Aufwand beim Vertragsabschluss und günstige Verwaltungskosten. Die Firma will eine ausgefeilte digitale Risikoanalyse für die Kundengewinnung einsetzen (Fromme, Digital wie Oscar, SZ 18.12.2015, 16).

Bayern

Mitarbeiterüberwachung im Bayern-Fanshop Oberhausen

Der Fußballclub Bayern München hat nicht nur Fans außerhalb von Bayern, sondern auch einen Fanshop in Oberhausen, zwischen Schalke und Dortmund, wo im November 2015 ein erweiterter Laden eingeweiht wurde. Ein Tag vor der Eröffnung des neuen Ladens verlangte der Betreiber des Einkaufszentrums eine Bescheinigung vom Fanschop-Betreiber, dass die installierten Überwachungskameras nicht gegen den Datenschutz verstoßen. Die Datenschutzbeauftragte des FC Bayern stellte diese Bestätigung umgehend aus, ohne sich die Überwachung vor Ort angeschaut zu haben und unter Zitieren einer nicht zutreffenden Rechtsgrundlage.

Eine dort beschäftigte Verkäuferin klagte vor dem Arbeitsgericht Oberhausen, weil zwei von elf Überwachungskameras den dortigen Sozialraum rund um die Uhr ins Visier nehmen und offenbar live nach München übertragen, nicht aber auf irgendein Gerät in Oberhausen. Im Sozialraum ziehen sich die Beschäftigten um und nehmen ihre Zwischenmahlzeiten ein. Dort sind aber auch zwei Tresore in die Wand eingelassen. Vor der Kamerainstallation waren die Beschäftigten nicht informiert worden. Die Bayern-Manager behaupten, damit Diebstahl verhindern zu wollen, was etwas unglaubwürdig ist, weil dort noch nie jemand in die Kasse oder in die Tasche einer KollegIn gegriffen habe. Der Sozialraum ist nach hinten mit einer schweren Stahltür gesichert, nach vorne mit einem Alarmmelder. Wer die Tür ohne Schlüssel öffnet, löst Alarm aus. Insbesondere nachdem der Umsatz stark gefallen ist, vermutete die Belegschaft, dass sie mit der Vollüberwachung unter Druck gesetzt werden solle.

Die klagende Verkäuferin, die seit 16 Jahren im Fanshop arbeitet, verlangte im Dezember 2015, dass die Kameras im Sozialraum abgebaut werden und drohte mit Klage. Nachdem nichts passierte, erhob sie Klage, weil es „keinen Winkel mehr“ gibt, der nicht überwacht ist und sie einen „Striptease vor laufender Kamera“ hinlegen müsse, wenn sie sich umzieht. Der Arbeitgeber ignorierte den anberaumten Prozesstermin und wurde am 07.01.2016 vom Arbeitsgericht in einem Versäumnisurteil zum Abbau verpflichtet. Statt aber die Kameras gemäß dem Urteil abzubauen, wurde dieses vom deutschen Fußball-Rekordmeister mit einem Einspruch angefochten. Es wurde behauptet, die beiden Kameras im Sozialraum hätten einen engeren Blickwinkel als die im Laden; bzgl. der Aufbewahrungszeit der Bilder war zunächst von 180 Tagen die Rede, dann von erheblich kürzer, ohne sich festzulegen. Ende Januar 2016 wurde der Filialleiter in Oberhausen nach fast 19 Jahren fristlos gekündigt, obwohl man ihn noch kurz zuvor als verdienten Mitarbeiter bezeichnet hatte. Er hatte sich in einem Brief an den Bayern-Vorstand – unter Bezugnahme auch auf die Kameras – über Arbeitsbedingungen auf dem „Niveau der untersten Kreisklasse“ beklagt (Dahlkamp/Latsch/Schmitt, Weiter Winkel, Der Spiegel 8/2016, 54-56).

Berlin

Digitales Inkassounternehmen „Pair“

Das Berliner Internetunternehmen Finleap will mit einem neuen Start-up die etablierte Inkassowirtschaft angreifen. Mit „Pair“, so der Name, will es säumige Zahlungspflichtige statt auf dem Postweg ausschließlich über E-Mail und SMS kontaktieren. Zudem will das Unternehmen mit Hilfe von Algorithmen herausfinden, warum eine KundIn nicht zahlt und wie sich am besten das Geld eintreiben lässt. Dabei sollen auch Daten zum Einsatz kommen, die eine SchuldnerIn in sozialen Netzwerken hinterlässt. Investor und Berater ist Sebastian Diemer, Mitbegründer des umstrittenen Hamburger Start-ups Kreditech (vgl. DANA 3/2013, 118), das Online-Kredite vergibt und dabei die Datenspuren der KundInnen im Netz auswertet (Digitale Geldeintreiber, Der Spiegel 7/2016, 72).

Nordrhein-Westfalen

Axa setzt auf Pay-as-you-drive und Digitalisierung

Mit dem neuen Programm will der Versicherer Axa (vgl. DANA 1/2015, 39 f.), dessen Deutschlandsitz in Köln ist, junge FahrerInnen locken. Wer unter 25 ist, kann damit bis zu 15% Rabatt erreichen. Die FahrerIn muss dafür eine Smartphone-App in einem Zeitraum von zwölf Wochen mindestens 40 mal für drei Kilometer oder mehr einschalten und hierbei einen guten Score erzielen. Ist die App auf dem Handy angeschaltet, misst sie Geschwindigkeit, Verhalten beim Bremsen, Beschleunigung und Kurvenfahren mit den Sensoren des Smartphones, also ohne Blackbox, im Auto. Nach der Fahrt wird der FahrerIn das Auswertungsergebnis angezeigt – die Strecke auf einer Karte und mit einzelnen dunkelrot markierten Punkten. Beispiel: „Kilometer 5,3: Viel zu starke Bremsung, Kilometer 9,78: Viel zu starke Beschleunigung.“ Der Score ist miserabel: 46 von 100 möglichen Punkten beim Beschleunigen, 45 Punkte beim Bremsen, nur beim Kur-

venfahren 64. „Gut“, lobt die App, aber nur da.

Damit bringt nach der Hannoveraner VHV (DANA 4/2015, 179) ein weiterer großer Autoversicherer einen Telematiktarif auf den Markt. Die Marktführer HUK Coburg und Allianz wollen 2016 folgen. Das Besondere an der Axa-App: Sie kommt ohne festverbaute Box aus und kann von der FahrerIn beliebig an- und ausgeschaltet werden, was die Anwendung für datenschutzbewusste FahrerInnen akzeptabler machen könnte als Systeme mit Dauerüberwachung. Kritisiert wird, dass das verwendete System das Fahrverhalten nur ungenau misst und deshalb ungeeignet sei. Axa sieht dies nicht so.

Für FahrerInnen unter 25 müssen die Versicherer mehr als doppelt so viel für Schäden ausgeben als für Versicherte zwischen 26 und 68. Dem Unternehmen wie auch anderen Anbietern geht es offenbar weniger darum, den individuellen Tarif personengenau zu berechnen, sondern darum, das Fahrverhalten zu beeinflussen. Dabei sollen Apps und Vergleiche als spielerische Verkehrserziehung mit FahrerInnen aus derselben Altersgruppe helfen.

Die Versicherer versuchen so, die Schadenlast durch junge FahrerInnen zu reduzieren. Zudem erlangen sie große Datenmengen über das Fahrverhalten, die langfristig in die Tarifierung einfließen können, und kommen mit ihren KundInnen öfter in Kontakt als bisher, wo sie nur einmal im Jahr die Rechnung herausschicken und danach nur bei einem Schaden gefragt sind.

Demselben Ziel dient auch das Pilotprojekt „Smartparking“, das die Axa in Düsseldorf testet. Mit App und Plastikkarte parken Versicherte des Unternehmens in den meisten Parkhäusern Düsseldorfs ohne Parkschein und Bargeld. Die AutofahrerInnen erhalten digital ständig eine genaue Übersicht, wo wie viele Plätze frei sind. Partner ist dabei das Start-Up Evopark.

Die klassischen Versicherungsunternehmen sehen ihre alten Geschäftsmodelle als bedroht an, weil Autohersteller in das Geschäft verstärkt einsteigen und Internetportale die bisherigen Vertriebswege in Frage stellen. Eine ganze Reihe von Start-ups bietet an, die ungeliebte Versicherung einfacher zu machen.

Axa-Deutschlandchef Thomas Buberl will mit Digitalisierung, Datenauswertung, Kostensenkung und Erhöhung der Kundenfrequenz die eigene Position retten: „Dafür brauchen wir auch andere Leute.“ Auch Umschulung sei wichtig. Die Mehrzahl seiner ProgrammiererInnen arbeite noch mit der Uralt-Programmiersprache Cobol, es gebe viele VersicherungsmathematikerInnen, aber wenig DatenanalystInnen. Außerdem zielt Buberl auf eine Flexibilisierung der Arbeitsplätze: „Wir brauchen keine festen Arbeitsplätze mehr“. Die belgische Schwester habe das vorgemacht. Das bisherige betriebliche Vorschlagswesen hat die Gesellschaft ersetzt: Wer eine gute Geschäftsidee hat, bekommt für die Umsetzung einen Etat und einen Arbeitstag pro Woche. Zwei Ideen wurden schon umgesetzt (Fromme, Das Smartphone fährt mit, SZ 04.12.2015, 20).

Thüringen

Schlecht geschredderte Krankenakten im Karnevals-Konfettiregen

Beim Straßenkarneval in Dermbach im Wartburgkreis sind zerschredderte Patientenakten als Konfetti unters Volk gebracht worden. Landesdatenschutzbeauftragte Lutz Hasse bestätigte am 03.02.2016, dass auf den nicht fachgerecht zerkleinerten Papierschnipseln personenbezogene Daten wie Namen, Adressen und Telefonnummern zu lesen waren. Eine Anwohnerin hatte beim Straßenfegen nach dem Karnevalsumzug zerschredderte Patientenunterlagen gefunden, auf denen der Name ihrer Schwester erkennbar war. Hasse kündigte ein Verwaltungs- und Bußgeldverfahren wegen des Verstoßes gegen Datenschutzrecht an.

Nach Angaben des Klinikums Bad Salzungen handelt es sich möglicherweise um Papiere aus einer Außenstelle des vom Klinikum betriebenen medizinischen Versorgungszentrums. Eine kurzfristig veranlasste Prüfung habe ergeben, „dass unter Missachtung der Vorschriften patientenbezogene Papiere nicht ordnungsgemäß entsorgt wurden“. Geschreddertes Material aus dem Versorgungszentrum in Kaltennordheim sei nicht bis auf die vorgeschriebene Endgröße zerkleinert und aus den Praxisräumen entfernt worden. „Die Vermutung liegt nahe, dass dieses von dort den Weg auf die Dermbacher Straßen fand.“ Im Klinikum selbst habe es keine Unregelmäßigkeiten gegeben, wie eine Überprüfung ergeben habe. Auf den in der Konfettikanone gelandeten Schnipseln sollen auch Namen der Ärzte erkennbar gewesen sein.

Das Krankenhaus hat den Landesdatenschutzbeauftragten nach eigenen Angaben unverzüglich über den Vorfall informiert. Hasse schickte noch am gleichen Tag zwei Mitarbeiterinnen nach Dermbach, um den Vorfall vor Ort zu untersuchen. Die Polizei ermittelt nach eigenen Angaben nicht wegen des Vorfalls. Es liege keine Strafanzeige vor. so ein Sprecher der Landespolizeiinspektion Suhl.

In Thüringen wird noch über den Skandal um ein wildes Aktenlager im nahe gelegenen Immelborn diskutiert. Dort waren im Sommer 2013 unter anderem auch sensible Unterlagen aus Arztpraxen gefunden worden. Die Umstände des Aktenfunds und die Rolle des Thüringer Datenschutzbeauftragten dabei beschäftigt einen Untersuchungsausschuss des Landtags (Karneval vs. Datenschutz: Patientenakten aus der Konfetti-Kanone, www.heise.de 11.02.2016).

Datenschutznachrichten aus dem Ausland

Dänemark

Kfz-Kennzeichen-Scanning stößt auf deutsche Kritik

Dänemarks Polizei richtet an den Grenzübergängen nach Deutschland und weiteren Verkehrsknoten, an insgesamt 24 Standorten, Kfz-Kennzeichen-Scangeräte ein, mit denen alle passierenden Autos erfasst werden. Das Justizministerium des Landes rechnet damit, dass ca. 30 Mio. Kennzeichen pro Jahr erfasst werden. Diese Daten werden mit Polizeiregistern abgeglichen, etwa um gestohlene Autos oder gesuchte Personen aufzufinden. Erklärte Zielsetzung ist die Bekämpfung der grenzüberschreitenden und der Banden-Kriminalität, aber auch das Aufspüren unversicherter Autos. Kennzeichendaten, bei denen es keine Treffer beim Abgleich mit Polizeidateien gegeben hat, werden nicht sofort, sondern erst nach 24 Stunden gelöscht, in besonderen Fällen, etwa zwecks Erstellung bestimmter polizeilicher Lagebilder, erst nach 30 Tagen.

Die Leiterin die Unabhängigen Landeszentrums für Datenschutz Schleswig-Holstein, Marit Hansen, die in dieser Frage sich mit ihren dänischen Kollegen austauschte, erklärte: „Aus deutscher Sicht ist diese umfassende und verdachtslose Vorratsdatenspeicherung problematisch“. Nach einem Urteil des Bundesverfassungsgerichts aus dem Jahr 2008 ist Kfz-Kennzeichen-Scanning in Deutschland nur erlaubt, wenn Daten bei Nicht-Treffern sofort spurenfrei gelöscht würden. Den Anlass für das Urteil hatte u. a. eine polizeirechtliche Regelung von Schleswig-Holstein gegeben. Bis auf die CDU wendeten sich sämtliche Fraktionen im Landtag von Schleswig-Holstein gegen die Überwachung, so z. B. der innenpolitische Sprecher der FDP Ekkehard Klug: „Es wird Bürger geben, die auf eine Fahrt nach Dänemark verzichten, sofern es für sie nicht unabdingbar ist.“ Der rechtspolitische Sprecher der Grünen Burkhard Peters meinte: „Ich halte das für eine Belastung der deutsch-dänischen Beziehungen. Wir erleben einen Rollback europäischer Freiheiten, der sich gewaschen hat“. Auch SPD-Innenpolitiker Kai Dolgner kritisierte, riet aber zu Zurückhaltung, „andere Länder an den eigenen Abwägungen zu messen“. Patrick Breyer von den Piraten kanzelte die Maßnahme als unverhältnismäßige Massenüberwachung ab. Der dänischen Überwachung vergleichbare Kontrollmaßnahmen an Hauptstraßen und Autobahnen gibt es auch in Frankreich, den Niederlanden, Belgien, Italien und Ungarn (Dänemark: Ab März wird jedes Auto digital erfasst, Schleswig-Holsteinische Landeszeitung 19.02.2016, 1, 4; Hiersemenzel, Minister wirft Dänemark Misstrauen vor, Kieler Nachrichten 20.02.2016, 11).

Schweiz

Überwachungsgesetz beschlossen

Das Schweizer Parlament hat am 18.03.2016 dem revidierten Gesetz zur Überwachung des Post- und Fernmeldeverkehrs (BÜPF) zugestimmt. KritikerInnen sehen in dem Gesetz eine massive Verschärfung der Überwachungsmethoden in der Schweiz. Es erlaubt den Einsatz von Staatstrojanern und „besonderen technischen Geräten“ bei der Ortung von Handys. In der Schlussabstimmung stimmten beide Kammern des Parlaments – der National- und der Ständerat – der Revision zu. Der Nationalrat sprach sich mit 160 zu 23 Stimmen bei 12 Enthaltungen dafür aus, der Ständerat mit 41 zu 4 Stimmen. Während die Mehrheit der Sozialdemokratischen Partei (SP) und der rechtspopulistischen Schweizer Volkspartei (SVP) mit „Ja“ stimmten, votierte die Fraktion der Grünen dagegen.

Für die Abstimmung waren im Vorfeld die letzten Differenzen zwischen den beiden Parlamentskammern aus Stände- und Nationalrat ausgeräumt worden. Eine sogenannte „Einigungskonferenz“ aus den beiden Räten hatte mehrheitlich dafür gestimmt, dass sog. „Telefonranddaten“ auch im Ausland gespeichert werden dürfen. Bei den Randdaten handelt es sich um die Verkehrsdaten wie die Dauer eines Telefonats und wer mit wem telefoniert hat. Es geht also um die Vorratsdatenspeicherung von Metadaten. Der Nationalrat hatte sich ursprünglich gegen das Speichern im Ausland und für eine Speicherung ausschließlich in der Schweiz ausgesprochen. Die Schweizer Justizministerin Simonetta Sommaruga hatte zuvor betont, dass das Schweizer Datenschutzgesetz auch dann gelte, wenn die Daten auf Servern im Ausland aufbewahrt würden. Eine Hürde war bereits zwei Wochen zuvor genommen worden, als sich nach dem Ständerat auch der Schweizer Nationalrat gegen die ursprünglich vorgesehene Ausweitung der Aufbewahrungsdauer von Vorratsdaten von sechs auf zwölf Monate ausgesprochen hatte.

Grundsätzlich ging es der Regierung, dem Bundesrat, bei der Revision darum, die gesetzlich erlaubten Überwachungsmöglichkeiten den aktuellen technischen Möglichkeiten anzupassen. Neu vorgesehen ist im überarbeiteten BÜPF der Einsatz von technischen Überwachungsgeräten wie beispielsweise IMSI-Catchern, aber auch von Abhör- und Richtmikrofonen. Beschlossen sind auch Antennensuchläufe, über die MobiltelefonbesitzerInnen und ihre Randdaten identifiziert werden können und die bereits häufig für Ermittlungen eingesetzt wurden. Gemäß Presseberichten hatten die Schweizer Strafbehörden im Jahr 2015 die Handy-Daten von 124 Antennen abgefischt.

Neu ist der Einsatz von „Staatstrojanern“ oder „Government Software“, kurz GovWare. Strafverfolgungsbehörden sollen die Trojaner in Computer einschleusen dürfen, um beispielsweise verschlüsselte Gespräche mit Skype und ähnlichen VoIP-Diensten mithören zu können. Erlaubt sein soll nicht die präventive Überwachung, sondern allein die Überwachung im Rahmen von

Strafverfahren. Staatstrojaner sollen nur zur Aufklärung schwerer Straftaten eingesetzt werden.

Der überwachungskritische Verein „Digitale Gesellschaft“ leitet aus dem Gesetz jedoch ab, dass Staatstrojaner auch zur Verfolgung von Bagatelldelikten eingesetzt werden können. Er kämpft mit einer Beschwerde beim Bundesverwaltungsgericht gegen die Vorratsdatenspeicherung. Diese soll gegebenenfalls bis zum Europäischen Gerichtshof für Menschenrechte (EGMR) weitergetragen werden. Die Schweizer Piratenpartei hat angekündigt, ein Referendum gegen die Änderungen in die Wege leiten zu wollen. Werden für ein solches Referendum 50.000 Stimmen gesammelt, könnte am Ende also das Stimmvolk über die Zukunft des neuen Überwachungsgesetzes entscheiden. Sie verweist darauf, dass das Gesetz den Quellenschutz für Ärzte, Anwälte und Journalisten aushebelt; der Einsatz von Staatstrojanern sei teuer und nutzlos (Sperlich, Schweizer Parlament stimmt Verschärfung des Überwachungsgesetz zu, www.heise.de 19.03.2016).

Schweiz

Datenschutzbeauftragter fordert Löschung von Bahnpassagierdaten

Der kommissarisch im Amt befindliche Schweizer Datenschutz- und Öffentlichkeitsbeauftragte (EDÖB) Jean-Philippe Walter verlangt von den Schweizer Bundesbahnen (SBB) und dem (Branchen-)Verband öffentlicher Verkehr (VöV) die Daten zu löschen, die bei Kontrollen des „Swiss Pass“ im Zug gesammelt werden. Dabei handelt es sich um eine Kundenkarte des VöV, die Sommer 2015 eingeführt wurde. Ohne sie können bei der SBB keine Abonnements oder Fahrausweise zum halben Preis erworben werden. Sie dient als Fahrausweis. Sehr viele SBB-KundInnen nutzen sie zudem für Partnerdienstleistungen wie etwa als Skipass oder für Programme zur Kundenbindung.

Walter kritisierte, dass die bei den Fahrscheinkontrollen durchgeführten Datenbearbeitungen keine gesetzliche Grundlage haben und zudem unverhältnismäßig seien. Bei kontrollierten Passagieren werden mit einem Lesegerät die Daten eines RFID-Chips auf dem Swiss Pass ausgelesen, online übermittelt und 90 Tage in einer Kontrolldatenbank aufbewahrt. Unter anderem werden die Uhrzeit, die Zugnummer und die Ausweisnummer des Swiss Pass gespeichert. Laut dem Datenschutzbeauftragten waren in der Datenbank Mitte Oktober 2015 – rund zweieinhalb Monate nach der Einführung des Swiss Pass – schon 3,2 Millionen Einträge gespeichert.

Walter berichtet, dass in den Medien „vor allem die Befürchtung ausgesprochen wird, dass aus den Kontrolldaten Bewegungsprofile erstellt werden könnten.“ Bei bestimmten Personen könne solch ein, wenn auch nicht detailliertes, Bewegungsprofil durchaus entstehen. Er habe auch viele Anfragen besorgter BürgerInnen erhalten und musste oft klarstellen, dass er das Projekt Swiss Pass weder genehmigt noch bewilligt habe.

Gemäss VöV und SBB dient die Kontrolldatenbank vor allem dazu, etwaige Kundenanliegen im Nachgang zu einer Reise zu beantworten. Auch die weiteren von SBB und VöV vorgebrachten Gründe überzeugten den Datenschutzbeauftragten nicht, weshalb er den VöV und die SBB aufforderte, die Kontrolldaten unverzüglich zu löschen und den Betrieb der Datenbank einzustellen. Laut Medienberichten haben die SBB ein offenes Ohr für den EDÖB: Der Datenschutz sei für die SBB zentral. Die Empfehlung des Datenschützers würden ernst genommen (Sperlich, Schweiz: Datenschützer fordert Löschung von Passagierdaten der Schweizerischen Bundesbahnen, www.heise.de 18.02.2016).

Frankreich

CNIL fordert per Bußgeld von Google weltweites Sperren von Inhalten

Die französische Datenschutzbehörde CNIL hat gemäß einer Mitteilung vom 24.03.2016 im Streit über das „Recht auf Vergessenwerden“ in Internet eine Geldstrafe von 100.000 € gegen Google verhängt. Europäische Datenschutzbehörden verlangen schon seit längerem, dass Google nach europäischem Recht beanstandete Suchergebnisse weltweit herausfiltert. Der Europäische Gerichtshof hatte im Mai 2014 entschieden, dass Suchmaschinen Links zu bestimmten Inhalten aus ihren Ergebnisseiten löschen müssen, wenn sich eine NutzerIn in ihren Persönlichkeitsrechten verletzt sieht. Mit dem Urteil blieben aber viele Detailfragen offen.

Google war der Kritik teilweise entgegengekommen und hatte angekündigt, die fraglichen Links im Land des Antragstellers auch auf nicht-europäischen Google-Seiten zu löschen. Werden also Treffer zum Beispiel auf Forderung einer Person aus Deutschland ausgeblendet, sind auch auf der bolivianischer Seite google.bo die beanstandeten Einträge in Deutschland nicht zu sehen – von Bolivien aus oder in anderen europäischen Ländern aber schon.

Dies genügt der CMIL mit Sitz in Paris nicht aus. Sie verweist unter anderem darauf, dass Internetnutzer diese Geo-Blockade mit technischen Mitteln umgehen könnten. Google kann gegen die Strafe Einspruch einlegen (Recht auf Vergessen: Französische Datenschützer verhängen Geldstrafe gegen Google, www.heise.de 24.03.2016).

Türkei

Wahlregister von 2008 im Internet veröffentlicht

Unbekannte haben personenbezogene Daten von über 49,6 Millionen türkischen BürgerInnen im Netz veröffentlicht. Darunter befinden sich der Name, die Adresse, Namen der Eltern, Geburtsdatum und -ort sowie die nationale Identifikationsnummer (Türkiye Cumhuriyeti Kimlik Numarası). Der Datensatz soll zuvor schon an Interessenten zum Kauf angeboten worden sein. Bei dem knapp 6,6 GB großen SQL-Dump ergaben stichprobenartige Prüfungen Übereinstimmungen mit echten Daten türkischer BürgerInnen. Allerdings scheint das Leak nur türkische BürgerInnen zu betreffen, die sich spätestens 2008 als Wähler registriert hatten. Mit den in der Datenbank enthaltenen Daten ist es nach Ansicht von türkischen Beobachtenden

möglich, Betrügereien zu Lasten der Opfer zu begehen. Besonders die nationale Identifikationsnummer eigne sich in Zusammenhang mit Geburtsdatum und Adresse oft, um sich als die jeweilige Person auszugeben. Auch lässt sich die Datenbank einfach zur Adressermittlung nutzen, vorausgesetzt die Person ist seit 2008 nicht umgezogen.

Vor dem öffentlichen Leak sollen die Daten bereits als verschlüsselte Datei die Runde gemacht haben und in dieser Form zum Kauf angeboten worden sein. Gegen Bezahlung habe man so mit einem speziellen Nutzerinterface einzelne Anfragen entschlüsseln können. Nun scheint jemand die gesamte Datenbank geknackt zu haben oder die ursprünglichen Hacker haben genug an der Datenbank verdient, um sie aus der Hand zu geben. Sicher scheint zu sein, dass die Daten aus dem Merkezi Nüfus İdaresi Sistemi (MERNİS) stammen, der zentralen Einwohnermelde-Datenbank der türkischen Regierung.

Augenscheinlich ist die Veröffentlichung politisch motiviert. Auf der Seite mit dem Datendump protestieren die Hacker gegen den türkischen Regierungschef Erdoğan und haben unter anderem dessen persönliche Daten als Beispiel hervorgehoben. Es ist aber auch von Donald Trump die Rede; und das in einer Formulierung, die den Eindruck erweckt, die Hacker wären aus den USA, wobei dies auch ein Verschleierungsversuch der wahren Motive der Täter sein kann (Scherschel, Persönliche Daten von 49 Millionen türkischen Wählern veröffentlicht, www.heise.de 04.04.2016).

USA

FBI gegen Apple – Kryptokontroverse unentschieden

- Der Gerichtsbeschluss

Am 29.03.2016 teilte das US-Justizministerium dem zuständigen US-Richter in Kalifornien mit, dass die US-Bundespolizei FBI die per Gerichtsanordnung eingeforderte Unterstützung des IT-Unternehmens Apple für die Entsperrung des Handys eines Straftäters „nicht länger benötigt“. Per Gerichtsanordnung hatte dieses zuvor Apple aufgefordert, FBI-Ermittlern dabei zu helfen, an Daten zu kommen, die auf dem iPhone 5C von Seyd Farook gespeichert sind. Farook hatte am 02.12.2015 gemeinsam mit seiner Frau Tashfeen Malik bei einer Weihnachtsfeier in San Bernadino 15 Menschen getötet, bevor beide bei einem Schusswechsel mit der Polizei selbst getötet wurden.

Zuvor hatten FBI-Experten zunächst erfolglos versucht, an die Daten heranzukommen. Sie wollen das Attentat rekonstruieren und herausbekommen, ob die beiden Komplizen hatten. Ihr Problem ist eine Technologie, die Apple und Google 2014, als Reaktion auf die Snowden-Enthüllungen, eingeführt haben: Mit iOS 8 beziehungsweise Android 5 führten beiden Firmen eine automatische Verschlüsselung des Handyspeichers ein. Diese Verschlüsselung lässt sich nur mit der korrekten PIN entsperren und lesbar machen. Früher ließen sich solche Sperren durch sogenannte Brute-Force-Angriffe überwinden: Man probierte einfach alle nur denkbaren Zahlenkombinationen durch, bis man die richtige findet. Dies funktioniert mit aktuellen iPhones nicht mehr. Zum einen blockiert eine Sperrfunktion das schnelle Ausprobieren von Zahlenkombinationen. Nach mehreren Fehlversuchen baut das System immer längere Pausen ein, sodass man schließlich mehrere Stunden warten muss, um den nächsten Code zu versuchen. Vor allem aber gibt es in iOS die Option, den Speicher nach zehn Fehlversuchen automatisch löschen zu lassen. Diese Option könnte beim Handy des Attentäters aktiviert worden sein. Die FBI-Experten haben ihre Versuche, die PIN zu erraten, offenbar eingestellt, um nicht Gefahr zu laufen, dass eben das passiert und möglicherweise nützliche Daten des Täters verloren gehen.

Gemäß der Gerichtsanordnung sollte Apple den Ermittlern helfen, „drei wichtige Funktionen bereitzustellen“:

1. Die automatische Löschfunktion sollte deaktiviert oder umgangen werden, egal ob sie aktiviert ist oder nicht.
2. Es sollte ermöglicht werden, Zahlencodes digital an das Handy zu übertragen, statt sie händisch auf dem Bildschirm eintippen zu müssen.
3. Es sollte sichergestellt werden, dass zwischen den vom FBI versuchsweise eingegebenen Zahlencodes keine Verzögerungen entstehen.

Mit anderen Worten: Apple sollte dem FBI helfen, den PIN-Code des iPhone 5C mit einem Brute-Force-Angriff zu knacken. Die Ermittler hatten auch konkrete Vorstellungen über das Vorgehen: Apple sollte eine iOS-Version bereitstellen, die die oben geforderten Funktionen enthält. Beim Aufspielen dieser Software sollte das bereits installierte iOS nicht verändert werden. Stattdessen sollte die Software im Arbeitsspeicher des Geräts installiert und so modifiziert werden, dass sie nur auf diesem einen Gerät lauffähig ist. Sollte der Konzern aber eine bessere Idee haben, wie die Aufgabe zu bewältigen wäre, dürfe er gern einen Vorschlag machen.

Da dieses Vorgehen mit einigem Aufwand verbunden gewesen wäre, wurde Apple in der gerichtlichen Anordnung aufgefordert, „angemessene Kosten“ zu nennen. Außerdem wurde Apple in Punkt 7 ermöglicht, binnen fünf Werktagen einen Antrag zu stellen, von der Anordnung entbunden zu werden, wenn es diese für „unzumutbar beschwerlich“ halte, was Apple dann auch tat.

- Die Reaktion Apples

Am 17.02.2016 veröffentlichte Apple-Chef Tim Cook einen offenen Brief an seine KundInnen. Man habe nach den Anschlägen von San Bernadino eng mit den Behörden zusammengearbeitet, bei den Ermittlungen geholfen und dem FBI alle geforderten Daten übermittelt. Sogar Apple-Ingenieure habe man als Berater bereitgestellt. Nun verlange die US-Regierung aber etwas, „das wir für zu gefährlich halten“: „Man hat uns aufgefordert, eine Hintertür für das iPhone zu bauen.“ Im Grunde sei es eine um wichtige Sicherheitsfunktionen bereinigte iOS-Version, die sich die Ermittler wünschen. „In den falschen Händen könnte diese Software – die es bis heute nicht gibt – potenziell jedes iPhone entschlüsseln.“ Eine Garantie, dass eine solche Software nur in diesem einen Fall genutzt würde, könne man nicht geben. Was das FBI fordere, „würde genau die Rechte und die Frei-

heit unterminieren, welche die Regierung beschützen soll".

Letztlich werde Apple aufgefordert, seine eigenen NutzerInnen zu hacken, seine eigenen Sicherheitsvorkehrungen zu schwächen und iPhone-AnwenderInnen hohen Risiken auszusetzen. Würde Apple tatsächlich dazu gezwungen, könnte die Regierung diese Schwäche ausnutzen, um „Ihre Nachrichten, Gesundheitsdaten und Finanzdaten abzufangen, Ihren Aufenthaltsort festzustellen oder sogar die Kamera und das Mikrofon Ihres iPhones unbemerkt zu aktivieren". Apple meinte zudem, ein Gericht in Kalifornien sei nicht der richtige Ort, um den Konflikt um die Verschlüsselung zu lösen und kündigte an, sich an den Kongress in Washington zu wenden.

Apples Position wurde von mehr als 30 Internet-Unternehmen, u. a. von Facebook, Google, Microsoft, Amazon, Ebay und Intel in einem Brief an das Gericht unterstützt. Sie verwiesen darauf, dass auch weniger demokratische Staaten das Knacken von Geräten verlangen könnten. Zudem könne der Vorgang ein juristischer Präzedenzfall sein, generell zum Einbau von Überwachungstechnik oder Hintertüren in ihre Geräte oder Software gezwungen zu werden. Unterstützung für Apple kam zudem von Yahoo, AT&T, Cisco, Box, Dropbox, Snapchat, Pinterest, Mozilla und Whatsapp. US-Staatsanwälte hatten schon signalisiert, dass sie viele, nicht nur von Terroristen stammende Handys, von Apple geöffnet bekommen wollen. In die Diskussion schaltete sich auch der UN-Hochkommissar für Menschenrechte Said Raad al-Hussein ein. Die US-Regierung riskiere, dass die „Büchse der Pandorra" geöffnet werde: „Ich ersuche alle Betroffenen, nicht nur auf den unmittelbaren Wert, sondern auch auf die potenziell größere Auswirkung zu achten."

Unterstützung kam auch von der US-Bürgerrechtsorganisation Electronic Frontier Foundation (EFF): „Sichere Software zu schreiben ist immer schwierig". Dies gelte vor allem für ein tief ins System eingreifendes Programm, das eng mit der Hardware interagiere. Bevor Apple eine solche Software signieren und freigeben könne, müsste der Konzern auch „strenge Tests" durchführen. Die EFF verglich die Anordnung mit einer Aufforderung an einen Autobauer, „einen neuen Lkw mit einem fünften Rad binnen eines Monats zu fertigen". Theoretisch wäre dies sicher möglich, würde aber viel Zeit und Geld verschlingen. Letztlich habe es sich in der Vergangenheit aber auch immer als „Sicherheitsalbtraum" herausgestellt, Backdoors zu bauen und Verschlüsselung zu umgehen, wie es das Gericht und die Regierung wünschten. Es sei auch davon auszugehen, dass das Crack-Programm nicht nur in dem einen Fall angewendet würde. Vielmehr sei das Drängen der Sicherheitsbehörden vorprogrammiert, die Software auf andere Geräte anzupassen und die Amtshilfe deutlich auszuweiten.

- Die Begehrlichkeiten der „Intelligence Community"

Apple legte es also auf eine Konfrontation mit der Regierung an und hoffte darauf, die öffentliche Meinung für sich gewinnen und die Regierung zu einer Umkehr bewegen zu können. Dass das FBI gerade zu diesem Zeitpunkt mit einer derartigen Forderung an Apple herantrat, war wohl kein Zufall. Die Behörde wollte offenbar die öffentliche Stimmung im Nachgang des Anschlags von San Bernardino ausnutzen. Gemäß Presseberichten soll Apple darum gebeten haben, die FBI-Anfrage nicht öffentlich zu stellen, so wie dies üblich ist. Im März 2016 liefen demnach in den USA neun Prozesse, bei denen es um das Entsperren von zwölf Apple-Geräten ging. Doch machte das FBI den San-Bernadino-Fall öffentlich und provozierte damit die deutliche Antwort von Apple-Chef Tim Cook.

Schon im August 2015 wurde von der Presse ein Schreiben von Robert Litt zitiert, der für das Büro des US-Geheimdienstdirektors arbeitet, worin er erklärt, dass das „legislative Umfeld" für Anti-Verschlüsselungs-Gesetzgebung derzeit zwar „sehr feindselig" sei, dass sich das aber „im Fall eines Terroranschlags oder eines Verbrechens ändern könnte, wenn dabei nachgewiesen werden kann, dass starke Verschlüsselung die Strafverfolger behindert hat".

Das Vorgehen des FBI war offenbar mit den übrigen Mitgliedern der „Intelligence Community" – also der Gesamtheit der US-Geheimdienste – abgesprochen. So gab CIA-Chef John Brennan der US-TV-Sendung „60 Minutes" eines seiner seltenen Interviews, in dem er behauptete, man habe „Tage vor" den Anschlägen von Paris im November 2015 erfahren, dass der „Islamische Staat" „eine Aktion durchzuführen versuchte". Die beteiligten Personen hätten jedoch „von neuen Kommunikationsmitteln Gebrauch machen können", die „den Strafverfolgungsbeamten verschlossen sind". Auf Nachfrage präzisierte Brennan: Ja, er spreche von Verschlüsselung. Belege blieb er in beiden Fällen schuldig. Tatsächlich konnte die Polizei die Attentäter damals offenbar abhören. Außerdem hatten die Ermittler anscheinend ohne Probleme ein Handy ausgewertet, das die Täter benutzt hatten.

In einer Replik auf den Einspruch von Apple erklärten die US-Justizvertreter, die Unterstützung durch Apple gegenüber dem FBI, „bedeutet nicht das Ende der Privatheit". Dass sich der IT-Konzern aus Cupertino dem Begehr entgegenstelle, beruhe scheinbar „auf seiner Sorge um sein Geschäftsmodell und seiner öffentlichen Marketingstrategie". Apple habe „zu keinem Zeitpunkt gesagt, dass es nicht die technischen Fähigkeiten habe, der Weisung Folge zu leisten". Bereits Anfang März 2016 schaltete sich der frühere NSA-Mitarbeiter und Whistleblower Edward Snowden in die Debatte ein und erklärte die FBI-Behauptung, ohne Apples Hilfe keinen Zugriff auf das Gerät bekommen zu können, für „Bullshit".

- Hilfe von Cellebrite?

Am 23.03.2016 berichteten Medien, dass das FBI zur Entsperrung des Handys des erschossenen Attentäters von San Bernardino die Hilfe der israelischen Firma Cellebrite in Anspruch nimmt. Die US-Bundespolizei hatte eine für für den Tag zuvor anberaumte Anhörung kurzfristig abgesagt, da eine „außenstehende Partei" dem FBI eine „mögliche Methode" zum Entsperren des Gerätes präsentiert habe. Cellebrite hat eine Technik namens Universal Forensic Extraction Device (UFED)

entwickelt, mit der Datenextraktion aus Mobilgeräten möglich sein soll, und bietet die eigenen Dienstleistungen Strafverfolgungsbehörden weltweit an. Nach eigenen Angaben besitzt die Firma die Fähigkeit, bestimmte iPhones und iPads mit iOS 8 zu entsperren – „ohne Hardware-Eingriff und dem Risiko einer Datenlöschung". Möglich ist dies angeblich nur bei älteren Geräten, darunter fällt aber auch das iPhone 5c aus San Bernardino, auf dessen Daten das FBI zugreifen will. Demnach hat die Firma inzwischen auch eine Methode gefunden, iOS 9 – zumindest auf älterer Hardware – zu entsperren. Deren Einsatz war, so die Nachricht des US-Justizministerium vom 29.03.2016, angeblich erfolgreich.

Cellebrite gehört seit 2007 zum japanischen Elektronikkonzern Sun Corporation. Das Unternehmen wirbt damit, „15.000 Nutzer in Strafverfolgung und Militär" zu haben. So ist nachvollziehbar, dass das Unternehmen der kroatischen Regierung Technik bereitstellte, um Kinderpornos auf sichergestellten Geräten zu finden. Auch die sächsische Polizei setzt Produkte von Cellebrite ein, um die 150 Handys, Laptops und Speicherkarten zu analysieren, die sie 2015 in einer umstrittenen Aktion auf einer linken Demonstration beschlagnahmt hatte. Das bayerische Landeskriminalamt kaufte Sommer 2015 14 UFED-Lizenzen von der Firma für 377.000 € incl. Wartung. Die deutsche Niederlassung von Cellebrite ist jüngst von Paderborn nach München umgezogen.

Später wurde in der Presse mitgeteilt, das FBI habe eine bei Hackern gekaufte Schwachstelle ausgenutzt, um das iPhone zu knacken. Es sei eine bisher unbekannte Sicherheitslücke gewesen, welche die Ermittler für eine Einmalzahlung mitgeteilt bekommen hätten. Die Dienste der Firma Cellebrite seien also nicht benötigt worden. FBI-Chef James Comey wurde zitiert, das bei dem iPhone 5c eingesetzte Verfahren funktioniere nicht bei neueren Modellen und auch nicht beim technisch etwas anspruchsvolleren iPhone 5s. Die Behörden hätten noch nicht entschieden, ob Apple über die Hacking-Methode unterrichtet werden soll, was dem Konzern die Möglichkeit geben würde, die Schwachstelle zu schließen.

- Offenlegungspflicht der Ermittlungsbehörden?

Diskutiert wird nun, ob das FBI seinen erfolgreichen Zugriff auf die Daten des iPhones und die dabei eingesetzte Methode gegenüber Apple offenlegen muss: Liegt eine Sicherheitslücke zugrunde, müsste diese möglicherweise von einem Gremium der US-Regierung geprüft werden. Es entscheidet, ob solche Schwachstellen geheimgehalten und von den Behörden ausgenutzt werden können – oder zur Sicherheit der Nutzer die betroffenen Anbieter informiert werden sollten.

Ein früherer Vize-Chef des Abhördienstes NSA erklärte gegenüber der Presse, die FBI-Methode sollte aus seiner Sicht diesem „Equities Review" unterworfen werden. Ein früherer ranghoher FBI-Experte für Cybersicherheit betonte jedoch, die Behörden seien nicht verpflichtet, Schwachstellen offenzulegen, wenn sie nicht weithin bekannt sowie nicht einfach zu missbrauchen seien. Gemäß Presseberichten hatte die Regierung bisher den Großteil der erkannten Sicherheitslücken offengelegt. So seien in einem Jahr nur etwa zwei von rund Hundert überprüften Schwachstellen zurückgehalten worden.

Sicherheitsforscher wie Jonathan Zdziarski spekulieren, dass für den Brute-Force-Angriff auf die iOS-Codesperre respektive PIN zur Spiegelung des NAND-Chips (NAND mirroring) gegriffen wurde. Dabei werden die verschlüsselten Daten des Flash-Speichers auf unterster Ebene dupliziert. Werden die Daten dann nach dem Durchprobieren mehrerer falscher PIN-Kombinationen automatisch gelöscht, könne man die Kopie wieder auf dem Original-Chip einspielen und das Prozedere von vorne beginnen. Auch sei denkbar, nur den Teil des Chips zu kopieren, auf dem die PIN-Eingabe-Versuche gespeichert werden. Nach mehreren erfolglosen Durchgängen könne dann die Originalversion wieder eingespielt und können die Versuche fortgesetzt werden (Kremp, iPhone-Entschlüsselung: Apple widersetzt sich FBI-Forderung, www.spiegel.de 17.02.2016; Martin-Jung, Code der Freiheit, SZ 18.02.2016, 1; Krempl, iPhone-Entsperrung: US-Justizministerium tut Apples Datenschutzkurs als Marketing ab, www.heise.de 20.02.2016; Apple will Kongress anrufen, SZ 22.02.2016, 19; Wir sind Apple, SZ 05./06.03.2016, 24; Boie, FBI will iPhone alleine knacken, SZ 23.03.2016, 7; Becker, Terroristen-iPhone: Israelische Firma hilft FBI angeblich beim Entsperren, www.heise.de 23.03.2016; Brühl, Codeknacker gegen Apple, SZ 24./25.03.2016, 25; Martin-Jung, Apple trotzt dem FBI, SZ 30.03.2016, 1; Hacker helfen FBI, SZ 14.04.2016, 9).

USA

Entschlüsselung von Smartphones bei FBI Routine

Die Ermittler des US-amerikanischen Justizministeriums verlangen nicht nur von Apple (siehe oben) Hilfe beim Entschlüsseln von Smartphones. Die Bürgerrechtsorganisation American Civil Liberty Union (ACLU) legte offen, dass das FBI auch Google dazu bringen will bzw. wollte, Zugang zu verschlüsselten Geräten zu erlangen. Nachdem bekannt geworden ist, dass Apple mindestens 70 Anordnungen nachgekommen ist, iPhones zu knacken, hat sich ACLU auf der Suche nach den Fällen gemacht und bisher in 22 US-Bundesstaaten 63 gefunden, bei denen die Ermittler seit dem Jahr 2008 nach dem All Writs Act von 1789 mit Hilfe des Anbieters auf verschlüsselte Daten zugreifen wollten. In mindestens neun Fällen war Google involviert. Dabei ging es hauptsächlich um Ermittlungen wegen Drogenvergehen.

Zu den 63 bestätigten Gerichtsverfahren kommen 13 weitere Fälle, die ACLU zu Gehör gekommen sind; 12 davon habe Apple erwähnt, allerdings seien deren Aktenzeichen nicht bekannt; in einem weiteren Fall gebe es zu wenig öffentliche Informationen. Die Bürgerrechtler kritisieren das FBI dafür, angegeben zu haben, den All Writs Act nur in besonderen Verfahren anzuwenden. Es habe sich gezeigt, dass dies fast zur Gewohnheit geworden sei. Die ACLU will ihre Recherchen fortsetzen (Wilkens, Auch Google soll dem FBI helfen, Smartphones zu knacken, www.heise.de 30.03.2016).

USA

New York etabliert WLAN-Netz ohne Datenschutz

New York will alle EinwohnerInnen und BesucherInnen der Stadt mit einem kostenloses Drahtlos-Netzwerk mit 10.000 WLAN-Säulen in Höchstgeschwindigkeit beglücken. Die Macher schwärmen schon jetzt von der „Telefonzelle von morgen.“ Die Einrichtung soll stadtweit in den nächsten acht Jahren erfolgen. Einheimische wie TouristInnen sollen sich mit ihrem Smartphone oder Tablet im Umfeld von 45 Metern zur Säule umsonst in das WLAN einloggen können; teils reicht das Signal bis zu 120 Meter weit. An USB-Anschlüsse zum Aufladen von Akkus wurde auch gedacht. Nicht nur für TouristInnen, die sich bei ihrem digitalen Stadtrundgang von Café zu Café hangeln müssen, um den Weg zum Museum oder Restaurant nachzuschlagen, soll den Service zugute kommen, sondern vor allem den New YorkerInnen selbst, die ihr Mobilgerät oft kaum aus der Hand legen und dauerhaft online zu sein scheinen: Mehr als ein Viertel aller Haushalte in der schnelllebigen Millionenmetropole haben laut einer Studie von Ende 2014 zu Hause keinen Zugang zum Breitband-Internet.

Selbst wer kein Smartphone hat, kann in New York an den drei Meter hohen Säulen über ein integriertes Display umsonst surfen, in einem Kartendienst nach dem Weg suchen oder umsonst innerhalb der USA telefonieren – per Lautsprecher oder dank Kopfhörer-Eingang auch mit Headset. Und: Wer auf den roten Knopf drückt, wird umgehend mit der Notrufzentrale verbunden. Die ersten Säulen in Manhattan laufen bereits, andere Stadtteile sollen folgen. 500 Stück sollen Sommer 2016 in Betrieb sein, mehr als 250 Geräte können einen Kiosk jeweils gleichzeitig nutzen.

Für DatenschützerInnen ist das kostenlose WLAN-Netz dagegen alles andere als eine Freude. Die zum Login notwendigen E-Mail-Adressen der UserInnen, besuchte Websites und Verweildauer auf bestimmten Inhalten werden gemäß der New York Civil Liberties Union (NYCLU) ab Login bis zu zwölf Monate gespeichert, wie sie in einem Brief an Bürgermeister Bill de Blasios Rechtsabteilung kritisiert. Da viele NutzerInnen sich täglich einloggen könnten, ließen Datenschutzrichtlinien sogar eine Hintertür offen, um die Daten letztlich auf unbestimmte Zeit zu speichern: „Eine massive Datenbank dieser Art schafft ein unangemessenes Risiko für Missbrauch und unerlaubten Zugang“. Die Gefahr besteht sowohl in möglichen Sicherheitslücken wie auch im uferlosen Zugriff durch Regierung und Polizei, so NYCLU-Direktorin Donna Lieberman: „Die privaten Online-Aktivitäten der New Yorker sollten nicht genutzt werden, um eine massive Datenbank in direkter Reichweite (der Polizei) NYPD zu erzeugen“. Die NutzerInnen gäben ihre politischen Ansichten, religiösen Überzeugungen oder Informationen über ihre Gesundheit und Familie preis.

Durch an den Säulen integrierte Kameras und sogenannte Umweltsensoren entsteht der Eindruck, dass das ohnehin schon stark überwachte New York einen weiteren Schritt in Richtung Big Brother macht. Weder die Kameras noch Sensoren, die etwa die Temperatur und Umgebungsgeräusche registrieren sollen, sind gemäß LinkNYC-Managerin Jen Hensley derzeit in Betrieb. Wann oder wofür genau sie eingesetzt werden sollen, sagt sie nicht.

Die NYCLU fürchtet, dass diese Informationen direkt an die Polizei oder das stadtweite System zur Terrorabwehr weiterfließen. Problematisch erscheint auch ein weiterer Aspekt: Hinter dem Konsortium Citybridge, das die Säulen mit digitalen Werbetafeln finanzieren will, steht unter anderem das Unternehmen Intersection. Das wiederum gehört zu Sidewalk Labs, das seinerseits von einem Konzern gegründet wurde, der wegen seiner riesigen Datenbestände schon lange in der Kritik steht und der seinen Kartendienst gleich mit in die Säulen verbaut hat: die Google-Muttergesellschaft Alphabet (Schmitt-Tegge, Datenschützer warnen vor kostenlosem WLAN in New York, www.heise.de 31.03.2016).

USA

Interministerieller Federal Privacy Council gegründet

Der US-Präsident Barack H. Obama hat eine Woche nach Verlautbarung zum EU-U.S.-Privacy-Shield Anfang Februar 2016 eine interministerielle Arbeitsgruppe, den Federal Privacy Council (Bundes-Datenschutzrat) geschaffen. Er soll das Vertrauen des Volkes in die Datenverwaltung der nationalen Behörden stärken sowie deren Datenschutz vereinheitlichen. Der Rat besteht zumindest aus den Datenschutzbeauftragten der Ministerien und anderer wichtiger Bundeseinrichtungen. In dem Anfang Februar 2016 erlassenen präsidentiellen Dekret heißt es: „Das ordentliche Funktionieren der Verwaltung braucht das Vertrauen der Öffentlichkeit. Und um dieses Vertrauen zu bewahren, muss die Verwaltung danach streben, die höchsten Standards für die Sammlung, Verwahrung und Verwendung personenbezogener Daten aufrechtzuerhalten. Datenschutz war ein Kern unserer Demokratie von Anfang an. Und wir brauchen ihn mehr als je zuvor.“ Er ordnete zudem die Ausarbeitung neuer Richtlinien und Anforderungsprofile für die höchsten Datenschutzbeauftragten der Bundeseinrichtungen an, was spätestens Anfang Juni 2016 erledigt sein soll.

Der Federal Privacy Council (FPC) tagt unter dem Vorsitz eines hochrangigen Beamten des Weißen Hauses und besteht aus mindestens 24 Mitgliedern. Darunter sind neben den höchsten Datenschutzbeauftragten der Ministerien etwa auch jener des Büros des Nationalen Geheimdienstdirektors, der NASA oder der Nationalen Wissenschaftsstiftung. Diese Einrichtungen sollen zudem Strukturen für eine bessere Zusammenarbeit miteinander schaffen. Der neue Datenschutzrat selbst soll sich mit einer Vielzahl anderer Räte koordinieren, zuforderst dem Federal Chief Information Officers Council. Statt Doppelgleisigkeiten wünscht der Präsident fruchtbare Zusammenarbeit und eine „effektive, effiziente und einheitliche Implementierung von Datenschutzrichtlinien in der gesamten Bundesverwaltung.“

Das Dekret nennt vier Funktionen des FPC: 1. Die Ausarbeitung von Empfehlungen für Datenschutzrichtlinien und -anforderungen, 2. die Koordination und das Teilen von Ideen, Best Practices, und Zugängen zu Datenschutz und für die Implementierung angemessenen Schutzes, 3. die Evaluierung von und Empfehlungen für die Bedürfnisse der Bundesverwaltung hinsichtlich Anstellung, Ausbildung und professioneller Weiterbildung in Datenschutzbelangen, und schließlich 4. die Durchführung anderer Funktionen mit Bezug zu Privatsphäre (von BürgerInnen) nach Vorgabe des Vorsitzenden (Sokolov, US-Datenschutz: Obama gründet Federal Privacy Council, www.heise.de 15.02.2016).

USA

Menschenbewertungsportal „Peeple“

In den USA ging die App „Peeple“ am 07.03.2016 im Web an den Start, mit der NutzerInnen andere Menschen bewerten können. Dafür müssen sie mit einem Facebook-Account bei „Peeple“ anmelden und können dann jede beliebige Person auf einer Skala von eins bis fünf bewerten. Dazu muss lediglich die Handynummer der zu bewertenden Person bekannt sein. Eine Einwilligung war zunächst nicht vorgesehen. Bewertete werden aber per SMS informiert, wenn ein Profil für sie eingerichtet wurde.

Die beiden Kanadierinnen Julia Corday und Nicole McCullough laden dazu ein, KollegInnen, NachbarInnen, Mieter, FreundInnen zu bewerten: „Wir wollen, dass der Charakter eine neue Art der Währung wird.“ Sie wollten mit ihrer App z. B. dabei helfen, gute BabysitterInnen auszuwählen. Außerdem könnten Freunde der eigenen Kinder auf Peeple online in Augenschein genommen werden. Positive Bewertungen gehen direkt online, negativen (zwei Sterne oder weniger) wird eine Wartezeit von 48 Stunden auferlegt. Gleichzeitig wird die bewertete Person informiert, um evtl. Differenzen mit den Verantwortlichen für die Bewertung auszuräumen. Gelingt dies nicht, wird die negative Bewertung freigeschaltet. Negative Bewertungen bleiben ein Jahr lang bestehen, bevor sie automatisch gelöscht werden. So hätten die Bewerteten die Möglichkeit, sich „zum Besseren zu verändern“.

Die Macherinnen haben insgesamt drei Kategorien vorgesehen, in die das Verhältnis zu den Bewertenden eingeordnet werden soll: beruflich, persönlich und romantisch. „Schlechtes Verhalten“ wie Beleidigungen werden in den Nutzungsbedingungen untersagt. Rassismus, Sexismus und Schimpfwörter sind gemäß den Teilnahmebedingungen verboten. Nutzende können Derartiges melden. Die Betreiber entscheiden dann, ob die NutzerIn und ihre Bewertung gesperrt wird. Die NutzerInnen selbst haben nur Einfluss auf Bewertungen und die zugehörigen Texte, die sie selbst verfasst haben.

Die beiden Gründerinnen bezeichnen ihre Software als „Positivity App“. Corday meint, es gehe bei ihrer App doch nur darum, öffentlich nett zueinander zu sein: „Wir wollen beweisen, dass die Welt gut ist und voller Menschen, die dich lieben.“ Als die Macherinnen ihre App im November 2015 ankündigten, bildete sich umgehend eine Gruppe „People vs. Peeple“ (Menschen gegen Peeple), der sich bis zum Webstart schon mehr als 12.000 Personen bei Twitter anschlossen. Hacker veröffentlichten alles, vom Gewicht bei der Geburt bis zu den Adressen, über die beiden Gründerinnen; es soll sogar Morddrohungen gegeben haben. Corday reagiert wie folgt: „Ich habe keine Zeit für meine Kritiker.“ Selbst Personen, die der Idee grundsätzlich aufgeschlossen gegenüber stehen, nahmen vom Start der App an Anstoß daran, dass zunächst keine Möglichkeit vorgesehen war, eine Bewertung zu untersagen. Statt von „Bewertungen“ spricht Peeple jetzt von „Empfehlungen“. Man müsse seinen Klarnamen angeben. Peeple-Nutzende können selbst entscheiden, welche Kommentare über sie freigeschaltet werden. Alles Negative lässt sich so verstecken. Die GründerInnen nennen dies „Reputationsmanagement“. Das Recht zum Verstecken negativer Bewertungen soll es nur vorübergehend geben. Das Start-up plant als Nächstes eine Bezahl-Variante, genannt „Lizenz der Wahrheit““. Wer zahlt, bekommt Zugang zu allen Bewertungen. Das Unternehmen hinter der App wurde schon zum Start gemäß Presseberichten auf 7,6 Mio. US-Dollar bewertet. Auf ihrer Homepage erklären die Macherinnen: „Egal ob ihr unser Konzept mögt oder nicht; wir heißen trotzdem jeden willkommen, dieses Online-Dorf voller Liebe und Überfluss für alle zu erkunden“ (Werner, Pranger-Portal, SZ 08.03.2016, 1; Holland, Peeple: Aufruhr um App zum Bewerten von Menschen, www.heise.de 01.10.2015).

USA

Firmen drängen Beschäftigte zu Gesundheitstests

Arbeitgeber in den USA bedrängen ihre Beschäftigten zunehmend, an firmeninternen Vorsorgeuntersuchungen, biometrischen Tests oder Gesundheitskursen, etwa zur Diabetes-Bekämpfung, zur Blutdrucksenkung oder zum Gewichtsabbau teilzunehmen. Grund ist nicht eine gesteigerte Fürsorge, sondern der Wunsch der Betriebe, die Prämienzahlungen für ihre Beschäftigten bei den privaten Krankenversicherungen zu drücken. Beschäftigte, die sich den Tests und Gesundheitsprogrammen verweigern, erhalten oft höhere Prämien auferlegt. Die Mehrkosten belaufen sich pro Kopf und Jahr auf mehrere Hundert, gelegentlich sogar auf einige Tausend Dollar. Nach Presseberichten haben renitente Beschäftigte sogar in Einzelfällen ihren Versicherungsschutz verloren.

Die staatliche Antidiskriminierungsbehörde EEOC sieht die Praxis, Beschäftigte mit finanziellen „Anreizen“ zur Teilnahme an Programmen zu drängen, kritisch. Sie befürchtet, dass die Unternehmen sensible Daten in die Hand bekommen, die Rückschlüsse auf potenziell teure Erkrankungen in der Zukunft erlauben. Diesen Beschäftigten könnte dann unter einem Vorwand gekündigt werden, was in den USA leichter möglich ist als z. B. in Deutschland. Der Versuch der EEOC, die Verhängung zu hoher Strafzahlungen und die Speicherung sehr sensibler Daten gerichtlich zu unterbinden, ist immer wieder erfolglos. So wies jüngst eine Bezirksrichterin in Wisconsin eine Klage gegen den Plastikproduktehersteller Flambeau mit der Begründung zurück, den Teilnehmenden an den Vorsorgeuntersuchungen drohe

kein Nachteil, weil ihr Arbeitgeber die Gesundheitsdaten der Beschäftigten nur anonymisiert speichere. Viele Betroffene sehen aber ihre Datenschutzrechte in Gefahr. Sie fürchten, dass die Betriebe sehr wohl auf individuelle Cholesterin-, Blutdruck- oder Zuckerwerte zurückgreifen können, um unliebsame oder potenziell teure Beschäftigte loszuwerden. So wird von Unternehmen z. B. registriert, wer raucht.

In Deutschland wäre ein solches Verhalten nicht möglich, da nicht der Arbeitgeber Vertragspartner der Krankenversicherung ist, sondern der Arbeitnehmer. Der Arbeitgeber hat i. d. R. keinen Zugriff auf Gesundheitsdaten der Beschäftigten. In den USA sind gut 80% der Beschäftigten sowie deren Familien über sog. Gruppenversicherungen abgesichert. Die Kosten werden entweder vom Unternehmen allein oder von beiden Beteiligten gemeinsam getragen. Nach Angaben des Amts für Arbeitsstatistik hatten bei der letzten Erhebung im Jahr 2014 ca. 69% der in der Privatwirtschaft Beschäftigten Anspruch auf einen Zuschuss zur Krankenversicherung. Im Durchschnitt übernahm der Arbeitgeber dabei 79% des Beitrags, so dass den Beschäftigten 21% blieben. Im öffentlichen Dienst ist die Zahl der Anspruchsberechtigten höher. Die EEOC plant im Frühjahr 2016 neue Richtlinien um sicherzustellen, dass Arbeitgeber Beschäftigte nicht zur Teilnahme an Vorsorgeuntersuchungen zwingen und die Gesundheitsdaten der Mitarbeitenden nicht zu deren Nachteil instrumentalisieren können (Hulverschmidt, Sensible Daten für den Chef, SZ 02.02.2016, 22).

USA

Hacking auf Gesundheitsdaten steigt massiv

Gemäß einer Studie des Ponemon Institutes waren 2014 Hacker-Attacken erstmals mit 45% der wichtigste Grund für Datenlecks im Gesundheitsbereich. Derartige Angriffe haben demnach seit 2010 um 125% zugenommen und somit andere Gründe für Datenverluste wie die Schlampigkeit von Mitarbeitern oder Diebstahl von Computern überflügelt. Bislang waren medizinische Daten vor allem durch Schlampigkeit wie verlorene Computer nach außen gedrungen. Im Jahr 2014 hatten 91% der befragten Organisationen im US-Gesundheitsbereich zumindest ein Datenleck zu beklagen. Medizinische Daten sind nicht nur kritisch, sondern für Cyberkriminelle auch viel wert. Seit der großen Gesundheitsreform von 2010 müssen in den USA die Daten von Krankenversicherten elektronisch gespeichert werden.

Eine Krankenakte soll laut Experten 60 bis 70 Dollar wert sein. Eine US-Sozialversicherungsnummer allein dagegen bringt auf dem Schwarzmarkt allenfalls einen Dollar. Unternehmen und Organisationen im Gesundheitsbereich waren bisher offenbar nicht gut auf Cyber-Bedrohungen vorbereitet. Larry Ponemon, Gründer und CEO des Ponemon Institutes meinte bei Vorstellung der Studie im Mai 2015: „Es gibt einige Ausnahmen, aber im Allgemeinen fehlen Healthcare-Anbietern entweder die Ressourcen, das Personal oder die technischen Neuerungen, um der sich wandelnden Cyberbedrohungs-Landschaft zu begegnen.“ Ann Patterson von der Verbraucherschutzorganisation Medical Identity Fraud Alliance begründete den Hype der Hacker: „Der Raub medizinischer Identitäten bringt Kriminellen heute erheblich mehr Geld ein als etwa der Klau von Bankdaten.“ Während sich Scheck- oder Kreditkarten bei einem Betrugsverdacht rasch sperren lassen, fällt der Diebstahl einer medizinischen Identität oft monatelang nicht auf. In dieser Zeit ordern die Diebe in großem Stil rezeptpflichtige Medikamente, die sie dann weiterveräußern, etwa an Drogensüchtige. Oder sie verkaufen die Identitäten an Kranke, die sich keine Versicherung leisten können. Wieder andere rechnen Leistungen ab, die niemand erhalten hat, oder erschwindeln staatliche Zuschüsse. Durch die Vermischung von echten und gefälschten Daten gelten Betroffene plötzlich als Drogenabhängige oder Raucher. Es kann zu Fehldiagnosen, Behandlungsfehlern oder anderen gravierenden Gesundheitsrisiken kommen, so Steve Weisgerber, Jura-Professor an der Bentley-University in Massachussetts: „Im schlimmsten Fall erhält jemand bei einem Unfall eine Bluttransfusion der falschen Blutgruppe, weil seine Daten geändert wurden.“ Ähnlich Rick Kam, Gründer des Studien-Sponsors ID Experts: „Medizinischer Identitätsdiebstahl ist 100 Mal schlimmer als Finanz-Identitätsdiebstahl“. Wenn ein Betrüger die medizinische Identität eines Opfers für eine Operation nutzt, könne die Krankenakte danach dessen Blutgruppe oder Medikamentenunverträglichkeiten auflisten statt jene des Opfers.

Neun von zehn Organisationen hatten laut „Fifth Annual Benchmark Study on Privacy & Security of Healthcare Data“ 2014 zumindest einen Vorfall, 40% sogar fünf oder mehr. Diese Datenlecks kosteten die Branche sechs Mrd. Dollar pro Jahr. Dazu kommen noch die Risiken für die Opfer, derer es laut der Studie 2014 bereits 2,3 Mio. gab. Erfährt die betroffene Person von dem Diebstahl, etwa bei der Quartalsmitteilung des Versicherers, hat sie oft größte Mühe, die korrekten und die fälschlich unter dem eigenen Namen abgerechneten Posten voneinander zu trennen. In 2/3 aller Fälle bleibt sie auf einem Teil des Schadens sitzen, was laut Ponemon Institute im Schnitt immerhin 13.500 Dollar waren (Pichler, Patientendaten: Hacker-Klau toppt Schlampigkeit, www.pressetext.com 08.05.2015; Hulverschmidt, Plötzlich drogensüchtig, SZ 25.02.2016, 1).

Ägypten

Überwachungs-Soft- und -Hardware von Hacking Team und Nokia

Die Menschenrechtsorganisation Privacy International (PI) berichtet, dass die italienische Firma Hacking Team im Jahre 2015 Überwachungssoftware nach Ägypten geliefert hat. Nokia wird in dem Bericht vorgeworfen, im Jahre 2011 ein Netzwerk für die Regierungskommunikation in Krisenzeiten geliefert zu haben (vgl. DANA 4/2015, 182 ff.). Während Nokia die Darstellung bestreitet, rechtfertigte bei Hacking Team der Pressesprecher Eric Rabe den Deal: Ägypten sei ein Land, dem Europa auch Kampfflugzeuge verkaufe.

Laut dem 20-seitigen Bericht von PI gibt es in Ägypten ein Technical Research Department (TRD), das von einer Frau mit dem Decknamen „Layla“ geleitet wird und dem Inlands-Geheim-

dienst Al-Mukhabarat Al-Amm zuarbeitet. Das TRD soll demnach eng mit zwei deutsch-ägyptischen Firmen namens Egyptian German Telecommunications Industries (EGTI) und Advanced German Technology (AGT) zusammengearbeitet haben, die bis ins Jahr 2015 hinein Software und Hardware zur Überwachung der Opposition importiert haben sollen. Außerdem hätte das TRD im Jahre 2011 über EGTI, einem Joint Venture zwischen der damaligen Nokia Siemens Network und einer ägyptischen Staatsholding, Netzwerktechnik eingekauft, um die Regierungskommunikation unabhängig vom öffentlichen Telefonnetz sicherzustellen, heißt es in dem Bericht.

In einem Brief an Privacy International bestätigt Nokia zwar die Lieferung von Komponenten, beruft sich aber auf einen „geerbten" Ausrüstungsvertrag, den Siemens im Jahre 2007 mit der damaligen Regierung Mubarak abgeschlossen habe. Nach der Erfüllung dieses Vertrages habe man keine weiteren Geschäftsbeziehungen nach Ägypten mehr unterhalten. Bezüglich der Software von Hacking Team verteidigte Firmensprecher Eric Rabe den Verkauf im Werte von knapp einer Million Euro: „Es ist vollkommen legal, Software nach Ägypten auszuführen. Ägypten ist ein Alliierter der USA, von vielen europäischen Ländern und sogar von Israel. ... Der Einsatz von Überwachungssoftware ist für uns alle im Kampf gegen den Terror wichtig" (Borchert, Überwachungs-Software für Ägypten, www.heise.de 27.02.2016).

Kuweit

DNA-Identifikation zur „Terrorbekämpfung" für alle

Im Rahmen eines neuen Anti-Terror-Gesetzes verabschiedete das kuwaitische Parlament im Juli 2015 ein weltweit einmaliges Gesetz mit der Nr. 78/2015, das alle 1,3 Mio. BürgerInnen und 2,9 Mio. BewohnerInnen verpflichtet, ihre DNA in eine nationale Datenbank eintragen zu lassen. Die Datenbank soll noch im Jahr 2016 realisiert werden und auch BesucherInnen erfassen. Bei Weigerung drohen ein Jahr Haft und eine Strafe von fast 30.000 Euro. Gibt jemand eine falsche Probe ab, drohen sieben Jahre Haft. Das Gesetz war nach einem Anschlag auf eine schiitische Moschee verabschiedet worden, bei dem 26 Menschen getötet und 227 weitere verletzt wurden. Ein Parlamentsabgeordneter erläuterte, man sei „zu fast allem bereit, was die Sicherheit in diesem Land verbessert".

Beamte des Innenministeriums erklärten, wieso die Datenbank keinen Angriff auf die Freiheit und Privatsphäre der Person darstelle. Kuwait ziehe lediglich gleich mit Staaten wie Großbritannien und den USA, die seit den 90er Jahren DNA-Proben für strafrechtliche Ermittlungen nutzen. Die Proben sollen durch mobile und stationäre Center gesammelt werden, die sich an staatlichen Einrichtungen und Büros befinden sollen. Dies ermögliche, „während diverser Erledigungen Proben abzugeben". Bei EinwohnerInnen, die keine Staatsbürgerschaft besitzen, sollen die DNA-Proben bei der Ausgabe oder Erneuerung ihres Visums gesammelt werden. Für BesucherInnen soll es im Flughafen Kuwait ein spezielles Center geben, in dem sie „zu ihren Rechten und Pflichten bezüglich des DNA-Gesetzes beraten werden". Dessen ungeachtet wird betont, dass für alle drei Gruppen die Abgabe von DNA-Proben verpflichtend ist.

Da Datenschutz „zweifellos das Hauptanliegen" des Innenministeriums sei, wurde in dem Gesetz geregelt, dass die Herausgabe von Informationen aus der DNA-Datenbank mit bis zu drei Jahren Haft geahndet werden soll, die Beschädigung der Datenbank mit mindestens drei, maximal zehn Jahren Haft. Es gebe strenge Auflagen für die BeamtInnen, die mit den Proben hantieren, sowie einen speziellen Mechanismus zur Erschwerung der Zuordnung von Proben zu ihren Quellen. Zudem gehe es nur um die nicht-codierenden Bereiche der DNA, die keine Rückschlüsse etwa auf eventuelle Krankheiten zulassen, und auch für Fragen der Abstammung soll die Datenbank nicht genutzt werden – dies „sichere das Gesetz".

Sarah Leah Whitson von Human Rights Watch reagierte mit dem Hinweis, viele Maßnahmen könnten potenziell nützlich gegen Terrorangriffe sein, aber ein potenzieller Nutzen sei keine ausreichende Rechtfertigung für massive Menschenrechtsverletzungen. Der Europäische Gerichtshof für Menschenrechte hatte 2008 entschieden, dass die Speicherung von DNA-Proben von Verdächtigen, die nicht verurteilt wurden, gegen Artikel 8 der Europäischen Menschenrechtskonvention verstößt (Jonjic, Kuwait errichtet DNA-Datenbank aller Einwohner, in Kalifornien wird „genetisch diskriminiert, www.netzpolitik.org 05.02.2016; Kuweit verlangt DNA-Test, SZ 28.04.2016, 42).

Technik-Nachrichten

Smartphone-Sensorik dient der Forschung , z. B. zur Erdbebendetektion

Forschende der University of California in Berkeley/USA planen, Mobiltelefone zu einem Netzwerk zu verknüpfen, um Erdbeben zu erkennen und die betroffenen Menschen frühzeitig zu warnen. Zusammen mit der Deutschen Telekom brachte das Berkeley Seismological Laboratory die App „MyShake" auf den Markt, die auf den Beschleunigungssensor von Smartphones zugreift. Sobald der eine Erschütterung feststellt, die für Erdbeben typisch ist, schickt das Gerät die Daten an einen Server in Kalifornien. Wenn 60% der mit MyShake ausgestatteten Smartphones im Umkreis von 10 km ebenfalls Alarm schlagen, vermutet das System ein Erdbeben und errechnet die Stärke. Wenn die laufenden Tests erfolgreich sind, soll tatsächlich

ein Alarm ausgelöst und an alle Telefone geschickt werden. Die App macht sich zunutze, das Smartphones Erdbeben ab einer Magnitude von 5 im Umkreis von 10 km registrieren. Neuere Modelle sind noch genauer. Die App ist in der Lage, Erdbeben von anderen Erschütterungen zu unterscheiden. Bei den Labortests mit Beispielsdaten erkannten die Geräte 2% der Erdbeben fälschlicherweise nicht. Umgekehrt waren 7% der Meldungen falscher Alarm. Je mehr Geräte in einem Gebiet mit der App arbeiten, umso seltener werden jedoch Fehler und umso genauer können Stärke und Epizentrum bestimmt werden.

Schon nach wenigen Tagen hatte Myshake Zehntausende Nutzende auf allen Kontinenten. Der Geophysiker Joachim Ritter vom Karlsruher Institut für Technologie meinte: „MyShake ist ein interessanter und Erfolg versprechender Ansatz“. Smartphones gebe es auch in Ländern, in denen kaum Echtzeit-Seismometer vorhanden sind, z. B. in Nepal, das 2015 von einem Beben der Stärke 7,8 betroffen war, oder Haiti, wo im Jahr 2010 Zehntausende Menschen in einem Beben der Stärke 7,0 ihr Leben verloren. Der Geophysiker Wolfgang Friedrich von der Ruhr-Uni Bochum kann sich vorstellen, mit den Handy-Daten „Shake Maps“ zu erzeugen, die die räumliche Verteilung der Bodenbewegungen darstellen: „Solche Karten könnten helfen, Rettungskräfte gezielt in die Gebiete größter Zerstörung zu leiten.“

Der von MyShake genutzte Beschleunigungssensor ist in den meisten Smartphones eingebaut. Damit erkennt das Gerät, in welche Richtung es ausgerichtet ist. Dazu wird die Wirkung der Schwerkraft in ein elektrisches Signal umgewandelt. Es gibt verschiedene Typen. Ein häufig verwendeter errechnet die Beschleunigung aus einer Änderung der elektrischen Kapazität. Für jede der Raumrichtungen enthält er einen wenige Mikrometer breiten Siliziumstab, der in die jeweilige Richtung frei beweglich ist. Wird das Gerät in eine Richtung beschleunigt, verändert sich aufgrund der Massenträgheit die Position des Stabs. Dieser bildet zusammen mit einer fest montierten Platte einen Kondensator. Dessen Kapazität ändert sich mit dem Abstand. Die elektrische Kapazität lässt sich leicht messen. Aus ihr lässt sich die Beschleunigung des Geräts berechnen.

Dieses Beschleunigungsmessen lässt sich auch für andere Forschungsfelder nutzen. So berechnet die App „Street Bump“ der Stadt Boston/USA während Autofahrten Erschütterungen, um Schlaglöcher zu lokalisieren. Je nach Fabrikat enthalten Smartphones auch ein Thermometer, ein Barometer, ein Hygrometer zur Bestimmung der Luftfeuchtigkeit sowie ein Magnetometer zur Messung von Magnetfelderm. Mit der in den Geräten installierten Kamera lassen sich nicht nur Fotos schießen; Forschende haben Verfahren entwickelt, mit denen anhand der erfassten Handybilder der Reifegrad einer Banane und der Chlorgehalt einer Wasserprobe bestimmt werden können. Ein Team der Nanyang Technological University in Singapur entwickelt eine App, die aus Handyfotos ablesen soll, wieviel Smog in der Luft ist.

Auch im medizinischen Bereich gibt es Anwendungen. Apple präsentierte im Jahr 2015 eine Schnittstelle namens „ResearchKit“, mit der Forschende iPhone-Apps für medizinische Studien entwickeln können. Zu den ersten Projekten gehörte „mPower“, das der Erforschung von Parkinson dienen soll. Diese App der nicht-kommerziellen Organisation Sage Bionetworks nutzt Touchscreen und Mikrofon von iPhones, um zu messen, wie stark Hände und Stimme von Probanden zittern. Teilnehmende sollen regelmäßig Übungen ausführen und dazu Fragen beantworten, etwa zu ihrer Ernährung, ihrem Schlaf und ihren sportlichen Aktivitäten. Aus der Kombination von Fragebogen- und Messdaten wollen die Forschenden neue Erkenntnisse über die Parkinson-Erkrankung gewinnen. Andere Apps auf der Grundlage von ResearcheKit sammeln Bewegungsdaten mithilfe des Beschleunigungssensors, um z. B. Diabetes, Herz- oder Atemwegserkrankungen zu erforschen.

Forschende überlegen, welche Messgeräte auf Handys noch gebraucht werden könnten. Ein Team vom Fraunhofer-Institut für Organische Elektronik, Elektronenstrahl- und Plasmatechnik und die TU Dresden entwickelt ein Spektrometer, das die chemische Zusammensetzung von Stoffen bestimmen kann und in ein Smartphone passt. Damit könnten Handynutzende selbst Lebensmittel auf ihre Inhaltsstoffe durchleuchten oder Luftschadstoffe messen. Sommer 2016 soll ein Prototyp fertiggestellt sein (Endt, Das Labor im Handy, SZ 24.02.2016, 12).

Hackerangriff auf Nissan Leaf erfolgreich

Auf der Mobile World Congress in Barcelona Ende Februar 2016 präsentierte Nissan sein Elektroauto „Leaf“ als das mobile Endgerät schlechthin – eine Art Smartphone mit Elektromotor, vier Rädern und einer intelligenten Schnittstelle, die Mensch und Maschine etwas enger verbinden soll. Wenige Tage später demonstrierte der Computerexperte und Sicherheitsforscher Troy Hunt, dass das Auto ohne große Probleme gehackt werden kann. Über die von ihm aufgedeckte Sicherheitslücke konnte nicht nur die BesitzerIn eines Nissan Leaf auf die IT des Autos zugreifen, sondern auch jedeR andere global über das Internet. Ein Hacker musste lediglich die richtige Internetadresse und eine Fahrzeug-Identifizierungsnummer parat haben. Beides ist nicht geheim: Die nötigen Webadressen kursieren im Netz, zum Beispiel in Foren, in denen sich besorgte Nissan-Leaf-HalterInnen über die Sicherheitslücke austauschen. Die Nummer ist links unten in der Windschutzscheibe für jeden sichtbar. Eine weitere Authentifizierung oder ein PIN-Code wird von der Schnittstelle Nissan-Connect-EV offensichtlich nicht abgefragt.

Um zu demonstrieren, welche Möglichkeiten das eröffnet, stellte Hunt ein Video ins Internet. Das zeigt ihn, nach eigener Aussage in Australien an seinem Computer sitzend, und seinen Partner, der in Nordengland in einem Nissan Leaf sitzt. Hunt kopiert sich eine URL in die Browserzeile – und ein paar Sekunden später springen die Sitzheizung und die Klimaanlage an, ohne dass der Partner am anderen Ende der Welt irgendetwas gemacht hätte. Kurze Zeit später schaltet Hunt die Systeme wieder aus und fragt Fahrdaten der vergangenen Tage ab: Datum und Uhrzeit, Strecke, verbrauchte Energie. Offenbar ist dabei die Zündung des Autos ausgeschaltet.

Es müsse angeblich nicht einmal eine konkrete Identifizierungsnummer bekannt sein, um an die Fahrdaten eines Nissan Leaf zu gelangen oder dessen Kli-

maanlage zu steuern, da sich die Nummern aller Nissan Leafs nur in den letzten fünf, maximal sechs Ziffern voneinander unterscheiden. Theoretisch sei es möglich, mithilfe von Programmen alle Ziffern durchzuprobieren, bis schließlich ein Treffer gelingt und ein Auto die gewünschten Daten sendet. Nissan bestätigte das Problem und teilte mit: „Connect EV steht unseren Kunden derzeit nicht zur Verfügung". Es seien aber weder sicherheits- noch fahrrelevante Funktionen betroffen (Harloff, Hacker drin, Klima läuft, SZ 26.02.2016, 21).

CDT warnt vor Profilbildung mit Sound Beacons

Die US-amerikanische Datenschutzorganisation Center for Democracy and Technology (CDT) warnt vor den Folgen von geräteübergreifendem Nutzer-Tracking mit Hilfe von der Werbung im Fernsehen oder im Internet unterlegten hochfrequenten Tönen, die Menschen nicht wahrnehmen. Tablets, Smartphones und Geräte in der Nähe können diese sogenannten Sound-Beacons registrieren und einem Benutzerprofil zuordnen. Damit könnten Werbenetzwerke auf breiter Front die Interessen des Nutzers auskundschaften und ihn geräteübergreifend mit zielgerichteter Werbung berieseln.

Die US-Aufsichtsbehörde Federal Trade Commission (FTC) hat sich am 16.11.2015 in einem Workshop mit dem Thema beschäftigt, wozu das CDT einen Bericht beisteuerte. Demgemäß entwickeln die Firmen Adobe, SilverPush, Drawbridge und Flurry an geräteübergreifenden Nutzerprofilen. Die US-Datenschützer warnen dabei besonders vor SilverPush. Im April 2015 habe man deren Software bereits in 6 bis 7 Apps gefunden. Ist eine solche App aktiv, kann sie das Sound-Beacon von Werbung identifizieren, die ein anderes Gerät abspielt. Laut SilverPush werde dabei nur auf die Beacons und nicht auf andere Geräusche oder gar auf Sprache gelauscht. Nach Angaben von CDT überwacht SilverPush so bereits 18 Millionen Smartphones (Kossel, Datenschutz: Werbe-Tracker überwinden Gerätegrenzen, www.heise.de 15.11.2015).

Rechtsprechung

BVerwG

Facebook-Fanpage-Verantwortlichkeit beim EuGH

Am 25.02.2016 beschloss das Bundesverwaltungsgericht (BVerwG) im Verwaltungsrechtsstreit zwischen der Wirtschaftsakademie Schleswig-Holstein GmbH (WAK) und dem Unabhängigen Landeszentrum für Datenschutz Schleswig-Holstein (ULD), die Frage der Verantwortlichkeit von Betreibern von Facebook-Fanpages für die Verarbeitung von Nutzungsdaten dem Europäischen Gerichtshof (EuGH) zur Beantwortung vorzulegen (1 C 28.14). Anlass war eine Anordnung des ULD gegenüber der WAK, einer Bildungseinrichtung der Industrie- und Handelskammer Schleswig-Holstein (IHK), vom 03.11.2011, eine von dieser betriebene Facebook-Fanpage zu deaktivieren. Nach Auffassung des ULD verletzt der Betrieb der Facebook-Fanpage europäisches und nationales Datenschutzrecht. Nachdem die WAK gegen die Anordnung Klage eingereicht hatte, beschäftigte der folgende Rechtsstreit bereits das Schleswig-Holsteinische Verwaltungsgericht (09.10.2013, DANA 4/2013, 169) und das Schleswig-Holsteinische Oberverwaltungsgericht (04.09.2014, DANA 4/2014, 184 f.).

Das Bundesverwaltungsgericht hat in seinem Beschluss keine Entscheidung über die maßgeblichen Rechtsfragen getroffen. Insbesondere die Verantwortlichkeit von Unternehmen für die Datenverarbeitung auf von ihnen betriebenen Facebook-Fanpages blieb ungeklärt. In der Verhandlung verwies der vorsitzende Richter Uwe Berlit auf einen Aufsatz von Martini/Fritzsche in NVwZ Extra 21/2015, 1 ff., dem sich der Senat inhaltlich weitgehend anschließen wolle. Das BVerwG legte insgesamt sechs Rechtsfragen zu Kernpunkten des zu entscheidenden Sachverhalts dem EuGH zur Beantwortung vor. Unter anderem will das BVerwG wissen, ob es neben den deutschen Regelungen zur Verantwortlichkeit weitere Umstände gibt, die für eine Verantwortlichkeit bei mehrstufigen Informationsanbieterverhältnissen Raum lassen. Speziell geht es hier um den Punkt, inwieweit es neben der Auftragsdatenverarbeitung eine Sorgfaltspflicht für die Auswahl von Dienstleistern im Internet gibt. Schließlich soll der EuGH klären, ob das Tätigwerden einer Datenschutzaufsichtsbehörde davon abhängig ist, dass vorher die für den Diensteanbieter zuständige Aufsichtsbehörde in einem europäischen Mitgliedstaat um eigenständiges Tätigwerden ersucht wird.

Bis zur Beantwortung der Fragen wird das Revisionsverfahren ausgesetzt. Marit Hansen, die Leiterin des ULD, hätte sich nach mehr als fünf Jahren und drei Gerichtsinstanzen klare Aussagen und einen Abschluss des Rechtsstreits gewünscht: „Vor dem Hintergrund, dass wir in zwei Jahren mit der Europäischen Datenschutz-Grundverordnung arbeiten werden, steht zu befürchten, dass der ursprüngliche Sachverhalt in der rechtlichen und technischen Umsetzung überholt sein wird." Mit der EuGH-Vorlage könnten sich aber evtl. neue deutlichen Impulse für den Schutz der Betroffenenrechte ergeben. Ähnlich Marcus Schween von der IHK: „Der Beschluss bringt leider noch nicht die erhoffte Rechtssicherheit für Unternehmen, die moderne Internetinfrastrukturen für geschäftliche Zwecke nutzen möchten" (ULD, PE 25.02.2016, Verantwortlichkeit von Fanpage-Betreibern vom Bundesverwaltungsgericht noch nicht entschieden - der EuGH soll‘s richten, https://www.datenschutzzentrum.de/artikel/1013-.html; IHK Schleswig-Holstein, PE 25.02.2016, EuGH hat das letzte Wort, www.ihk-schleswig-holstein.de).

BGH

Bewertungsportale unterliegen Prüf- und Begründungspflichten

Der Bundesgerichtshof (BGH) hat mit Urteil vom 01.03.2016 die Vorausset-

zungen für die Bewertung von Ärzten im Internet präzisiert (VI ZR 34/15). Ein Zahnarzt hatte gegen die Betreiberin von www.jameda.de, ein Portal zur Arztsuche und -bewertung, geklagt, weil er sich von einer ihm anoym bleibenden Person ungerecht negativ bewertet fühlte. Die Bewertung, die die Nutzenden ohne Angabe seines Klarnamens abgeben können, erfolgt dabei anhand einer sich an Schulnoten orientierenden Skala für insgesamt fünf vorformulierte Kategorien, namentlich „Behandlung", „Aufklärung", „Vertrauensverhältnis", „genommene Zeit" und „Freundlichkeit". Ferner besteht die Möglichkeit zu Kommentaren in einem Freitextfeld.

Der Kläger war mit der Gesamtnote 4,8 bewertet worden mit dem Zusatz „Ich kann Dr. I. nicht empfehlen". Die 4,8 war aggregiert worden u. a. aus den Noten „6" für „Behandlung", „Aufklärung" und „Vertrauensverhältnis". Der Kläger bestreitet, dass er den Bewertenden behandelt hat und hatte Jameda vorprozessual zur Entfernung der Bewertung aufgefordert. Diese sandte die Beanstandung dem ihm bekannten Nutzenden; dessen Antwort leitete Jameda dem Kläger unter Hinweis auf datenschutzrechtliche Bedenken nicht weiter. Die Bewertung blieb online.

Der Zahnarzt forderte mit seiner Klage die Unterlassung der Verbreitung der Bewertung. Das Landgericht Köln hatte zuvor mit Urteil vom 09.07.2014 der Klage stattgeben (28 O 516/13); das Oberlandesgericht (OLG) Köln hatte sie auf die Berufung der Beklagten hin am 16.12.2014 abgewiesen (15 U 141/14). Der für das allgemeine Persönlichkeitsrecht zuständige 6. Zivilsenat des BGH hob diese Entscheidung auf und verwies den Rechtsstreit an das Berufungsgericht zurück. Die beanstandete Bewertung sei keine eigene „Behauptung" von Jameda, weil sie diese sich nicht inhaltlich zu eigen gemacht hat. Die Beklagte hafte für den von Nutzenden ihres Portals abgegebene Bewertung deshalb nur dann, wenn sie zumutbare Prüfungspflichten verletzt habe. Deren Umfang richtet sich nach den Umständen des Einzelfalles. Maßgebliche Bedeutung komme dabei dem Gewicht der beanstandeten Rechtsverletzung, den Erkenntnismöglichkeiten des Providers sowie der Funktion des vom Provider betriebenen Dienstes zu. Hierbei dürfe einem Diensteanbieter keine Prüfungspflicht auferlegt werden, die sein Geschäftsmodell wirtschaftlich gefährdet oder seine Tätigkeit unverhältnismäßig erschwert.

Jameda habe diese ihr obliegenden Prüfpflichten verletzt. Bewertungsportale trügen ein gesteigertes Risiko von Persönlichkeitsrechtsverletzungen in sich, was sich durch die Möglichkeit, Bewertungen anonym oder pseudonym abzugeben, verstärke. Dem betroffenen Arzt sei es bei derart verdeckt abgegebenen Bewertungen schwer, gegen den Bewertenden direkt vorzugehen. Vor diesem Hintergrund hätte die beklagte Portalbetreiberin die Beanstandung des betroffenen Arztes dem Bewertenden übersenden und ihn dazu anhalten müssen, ihr den angeblichen Behandlungskontakt möglichst genau zu beschreiben. Darüber hinaus hätte sie den Bewertenden auffordern müssen, ihr den Behandlungskontakt belegende Unterlagen, wie etwa Bonushefte, Rezepte oder sonstige Indizien, möglichst umfassend vorzulegen. Diejenigen Informationen und Unterlagen, zu deren Weiterleitung sie ohne Verstoß gegen § 12 Abs. 1 TMG in der Lage gewesen wäre, hätte sie an den Kläger weiterleiten müssen. Im weiteren Verfahren werden die Parteien Gelegenheit haben, zu von der Beklagten ggf. ergriffenen weiteren Prüfungsmaßnahmen ergänzend vorzutragen.

Der BGH schützt also die Anonymität der Bewertenden, gibt aber den Bewerteten bessere Möglichkeiten, sich zur Wehr zu setzen. Im Juli 2014 hatte der BGH gegen einen Arzt entschieden, der im Portal Sanego negativ bewertet wurde, weil er angeblich im Wartezimmer lange warten ließ und ein falsches Medikament verschrieben habe. Der BGH signalisierte, dass die freie Meinungsäußerung Bewertungen zulasse, die ein Arzt ertragen müsse. Jetzt klärte der BGH, dass der betroffene Arzt das Recht hat, mehr über denjenigen zu erfahren, der die Bewertung abgegeben hat, Und die Tatsacheninstanz des OLG muss prüfen, ob Jameda abgeklärt hat, dass der Bewerter wirklich in Behandlung war. Umgekehrt hat der Arzt ein berechtigtes Interesse, der Sache nachzugehen.

Jameda-Geschäftsführer Florian Weiß zeigte sich zufrieden. Den konkreten Fall habe man geprüft. Aus Rücksicht auf den Bewerter habe man aber die Unterlagen nicht herausgegeben: „Jetzt wissen wir, dass wir in einem solchen Fall Unterlagen erfragen und sie geschwärzt weitergeben sollen". Reagiert ein Bewerter nicht auf eine Rückfrage, werde der Kommentar gelöscht. Jameda wolle nicht Hetze und Verleumdung Vorschub leisten. „Aber wir glauben, dass Ärztebewertungen nur anonym zustande kommen." Jameda hat im Jahr 2015 6 Mio. Euro umgesetzt und 2 Mio. Euro Gewinn vor Steuern erwirtschaftet. Alle ca. 280.000 niedergelassenen ÄrztInnen sind hier zu finden, ebenso HeilpraktikerInnen und PhysiotherpeutInnen. Nach Angaben von Jameda besuchen jeden Monat 5,5 Mio. Menschen das Portal. Jeden Tag kommen 1.500 Posts zu den mehr als 1 Mio Bewertungen hinzu. Eine Software soll hämische Auswüchse aussortieren. Der Rest geht direkt online. D. h. die Betroffenen müssen sich selbst zur Wehr setzen (BGH, PE Nr. 49/16 v. 01.03.2016, Bundesgerichtshof konkretisiert Pflichten des Betreibers eines Ärztebewertungsportals; Berndt, Krank geschrieben, SZ 02.03.2016, 10).

VG Hannover

Keine datenschutzrechtliche Anordnungsbefugnis bei öffentlichen Unternehmen

Das Verwaltungsgericht (VG) Hannover hat mit Urteil vom 10.02.2016 auf die Klage der üstra Hannoversche Verkehrsbetriebe AG eine datenschutzrechtliche Verfügung der Landesbeauftragten für den Datenschutz Niedersachsen (LfD Nds.) aufgehoben (Az. 10 A 4379/15). Mit dieser Verfügung hatte die LfD Nds. die Einstellung der Videoüberwachung in Bussen und Bahnen angeordnet, solange die üstra AG kein datenschutzkonform abgestuftes Überwachungskonzept vorlege oder anhand einer konkreten Gefahrenprognose nachweise, dass die bisher praktizierte flächendeckende Videobeobachtung erforderlich sei.

Das VG gab der Klage statt, ohne die zwischen den Beteiligten streitige datenschutzrechtliche Rechtmäßigkeit der Videoüberwachung als solche zu beurtei-

len. Die Verfügung erweise sich schon mangels ausreichender Rechtsgrundlage als rechtswidrig. Die LfD Nds. könne sich dafür nicht auf das Bundesdatenschutzgesetz (BDSG) stützen. Die üstra AG nehme mit dem Betrieb des öffentlichen Personennahverkehrs hoheitliche Aufgaben der öffentlichen Daseinsvorsorge wahr und sei insofern öffentliche Stelle im Sinne des BDSG. Auf öffentliche Stellen in den Ländern sei das BDSG aber nur unter weiteren, hier nicht gegebenen Voraussetzungen anwendbar. Eine Rückverweisung aus dem Niedersächsischen Landesdatenschutzgesetz (LDSG) in das BDSG gebe es nicht. Nach dem insofern im Rechtsverhältnis der Beteiligten zueinander allein einschlägigen LDSG habe die LfD Nds. nicht dieselben Eingriffsbefugnisse wie nach dem BDSG; insbesondere könne sie eine für datenschutzwidrig gehaltene Praxis nicht untersagen, sondern lediglich beanstanden. Die ausdrücklich auf die Einstellung der derzeitigen Praxis gerichtete Verfügung sei schon deshalb aufzuheben. Die zwischen den Beteiligten streitige Frage, wie die Videoüberwachung nach dem BDSG zu beurteilen wäre, stelle sich nach alledem in diesem Gerichtsverfahren nicht. Die Kammer hat gegen das Urteil wegen grundsätzlicher Bedeutung die Berufung zum Nds. Oberverwaltungsgericht zugelassen (VG Hannover: Keine Befugnis der Landesdatenschutzbeauftragten zur Untersagung der Videoüberwachung in den Fahrzeugen der üstra, www.heymanns-download.de 11.02.2016, VG Hannover, PM 10.02.2016).

LG München

Keine Werbevertrag bei kostenloser Online-Zeitung

Die Zivilkammer des Landgerichts (LG) München hat mit Urteil vom 22.03.2016 eine Klage des Süddeutschen Verlags gegen die Kölner Firma Eyeo abgewiesen, mit dem dieser den Vertrieb des Werbeblockers Adblock Plus unterbinden wollte (Az. 33 O 5017/15). Der Verlag wirft Eyeo vor, den Vertrieb von Werbung auf der Website süddeutsche.de gezielt zu behindern und so jährlich Schäden im „mittleren sechsstelligen Euro-Bereich“ zu verursachen. Eyeo greife in den impliziten Vertrag zwischen Verlag und LeserInnen ein, der die Anzeige kostenlos abrufbarer Artikel vorsehe.

Eyeo hingegen meinte, seine Software diene dazu, dass die Nutzenden ihre informationelle Selbstbestimmung durchsetzen könnten. Nur wenn sie Adblocker und ähnliche Programme verwenden, könnten sie verhindern, dass die Werbeindustrie sie trackt oder Webserver schädliche Programme aufspielten. Zudem stehe es dem Verlag frei, seine Inhalte anders zu monetarisieren. Eyeo sei auch nicht daran interessiert, die Werbefinanzierung komplett zu unterbinden, da das Unternehmen in seinem Acceptable-Ads-Programms an den Werbeumsätzen der Vertragspartner beteiligt sei.

Die Richter stellten gemäß der Verlagsargumentation fest, dass Eyeo und der Süddeutsche Verlag tatsächlich konkurrierten, wodurch nach dem Wettbewerbsrecht geklagt werden könne. Dieser Punkt war bei vorangegangenen Klagen anderer Medienhäuser strittig. Doch sah das LG keine gezielte Behinderung des Süddeutschen Verlags. Es gebe auch kein faktisches Vertragsverhältnis, das die LeserInnen verpflichte, Werbung anzuschauen.

Der Werbeblocker stelle keinen tiefen Eingriff in die Kommunikation zwischen Verlag und LeserInnen dar. Der Verlag hatte argumentiert, dass der Werbeblocker nicht nur Werbung, sondern auch Copyright-Hinweise und Links auf das Impressum entfernt habe. Dies erklärte Eyeo damit, dass die betroffenen Bereiche vom Verlag technisch als Werbung gekennzeichnet gewesen seien; die Filter seien korrigiert worden.

Die Entscheidung kommt nicht überraschend. Zuvor hatten bereits Landgerichte in Hamburg, Köln und München für Eyeo entschieden. Mehrere Medienhäuser haben bereits angekündigt, den Streit durch den Instanzenweg zu führen. Sie erhoffen vom Bundesgerichtshof eine Korrektur der Entscheidung in Sachen „Fernsehfee“, durch die Werbeblocker prinzipiell für legal erklärt wurden. Medienhäuser gehen auch auf anderer Ebene gegen Adblocker vor. So hatte der Verlagskonzern Axel Springer zumindest die Verbreitung von Filterregeln unterbinden lassen, die die Umgehung der auf bild.de eingesetzten Adblocker-Sperre ermöglichen.

Immer mehr Webseiten greifen wegen der zunehmenden Verbreitung von Adblockern und Anti-Tracking-Techniken mittlerweile zu technischen Gegenmaßnahmen: Sie sperren die NutzerInnen solcher Programme von ihren kostenlosen Angeboten aus oder fordern sie zumindest auf, bestimmte Websites freizuschalten. Französische Verleger haben eine gemeinsame Aktion zur Blockade von Adblockern gestartet; in Schweden ist Ähnliches in Vorbereitung. Paywalls werden immer verbreiteter. So sind seit 2015 auch viele Inhalte auf süddeutsche.de zahlenden KundInnen vorbehalten (Kleinz, Werbeblocker: Eyeo gewinnt vor Gericht gegen „Süddeutsche Zeitung“, www.heise.de 30.03.2016).

LG Berlin

Ordnungsgeld gegen Facebook wegen ungenügender AGB-Änderung

Gemäß einem Beschluss des Landgerichts (LG) Berlin vom 11.02.2016 muss Facebook 100.000 Euro Ordnungsgeld in die Staatskasse überweisen, weil das Unternehmen gegen eine Unterlassungsverpflichtung des höherinstanzlichen Kammergerichts Berlin (KG) verstoßen hat (16 O 551/10). Facebook habe anders als vom KG gefordert eine Passage in den Vertragsklauseln zwischen dem sozialen Netzwerk und seinen deutschen NutzerInnen nicht ausreichend abgeändert.

Ursprung dieses Verfahrens ist eine Klage der Verbraucherzentrale Bundesverband (vzbv) gegen Facebook aus dem Jahr 2010. Die Verbraucherschützer hatten moniert, dass die sogenannte „IP-Lizenz-Klausel“ in Facebooks Nutzungsbedingungen zu unbestimmt formuliert sei und sich damit nachteilig auf die deutschen NutzerInnen auswirke. Mit dieser „IP-Lizenz“ räumt sich Facebook nichtexklusive, weltweite Rechte zur Verwendung aller Inhalte ein, die Mitglieder des Netzwerks dort posten (IP steht in diesem Fall für „Intellectual

Property“). Der vzbv hatte in dem Verfahren in erster und zweiter Instanz Recht bekommen. Das KG warf Facebook vor, mit der Klausel gegen das Transparenzgebot zu verstoßen und untersagte deren Nutzung mit Beschluss vom 24.01.2014 (5 U 42/12). Nach der Zurückweisung einer Nichtzulassungsbeschwerde des Bundesgerichtshofs (BGH) ist dieses Urteil seit Oktober 2015 rechtskräftig. Im Dezember 2015 prüfte der vzbv, ob sich Facebook an die Unterlassungsverpflichtung hält. Man fand eine geänderte, aber nach Ansicht des vzbv immer noch rechtswidrige Version der Klausel vor und beantragte ein „in das Ermessen des Gerichts gestelltes Ordnungsgeld bis zu 250.000 Euro“.

Das LG Berlin folgte der Argumentation des vzbv. Die neue Klausel sei im Kern nicht konkreter, damit verstoße Facebook gegen die Unterlassungsverpflichtung. Zwar habe Facebook bereits angekündigt, die Klausel demnächst nochmals ändern zu wollen, dies könne sich aber nicht mehr auf den Verstoß auswirken: „Die Beibehaltung einer Klausel mit dem gerichtlich beanstandeten Inhalt lässt erkennen, dass die Schuldnerin das gerichtliche Verbot nicht ausreichend ernst genommen hat.“ Die vergleichsweise hohe Summe von 100.000 Euro für ein erstes Ordnungsgeld erklärt das Gericht damit, dass die Sanktion „auch für die wirtschaftlich starke Schuldnerin zumindest spürbar sein“ müsse.

Klaus Müller, Vorstand des vzbv, zeigte sich mit dem noch nicht bestandskräftigen Beschluss zufrieden: „Facebook versucht sehr beharrlich, Verbraucherrechte in Deutschland und Europa zu umgehen. Ein Ordnungsgeld von 100.000 Euro ist ein deutliches Signal. Unternehmen müssen gerichtliche Entscheidungen umsetzen und können sie nicht einfach aussitzen. Eine AGB-Klausel werde nicht dadurch besser, dass Facebook ein paar Worte ändere. Ein Sprecher von Facebook erklärte dazu, dass das Unternehmen die Zahlung des Ordnungsgeldes akzeptiere (Bleich, LG Berlin: Facebook muss 100.000 Euro Ordnungsgeld zahlen, www.heise.de 29.02.2016).

LG Düsseldorf

„Like“-Button ohne Info und Einwilligung unzulässig

Das Landgericht (LG) Düsseldorf hat der Klage der Verbraucherzentrale Düsseldorf (VZ NRW) wegen des „Gefällt mir“-Buttons von Facebook mit Urteil vom 09.03.2016 gegen den Bekleidungshändler Peek & Cloppenburg weitgehend stattgegeben (Az. 12 O 151/15). Die VZ hatte kritisiert, dass durch das Plugin Daten, die über das Surfverhalten des Kunden Auskunft geben, schon beim einfachen Aufrufen einer Seite an Facebook weitergeleitet werden. Das LG entschied, dass Unternehmen die SeitenbesucherInnen über die Weitergabe von Daten aufklären müssen. Die Integration des „Like“-Buttons verletze Datenschutzvorschriften, weil dadurch unter anderem die IP-Adresse des Nutzers ohne ausdrückliche Zustimmung an Facebook weitergeleitet werde. Dies passiert unabhängig davon, ob die Seitenbesucherin Facebook-Mitglied ist oder nicht. Eine Information wurde nicht gegeben noch um eine Einwilligung gebeten.

Rechtsanwältin Sabine Petri von der Verbraucherzentrale zeigte sich mit dem Urteil zufrieden und kommentierte: „Keiner weiß, was Facebook mit den Daten macht“. Unternehmen könnten sich nicht einfach aus der Verantwortung ziehen, indem sie auf Facebook verweisen.

Bei Peek & Cloppenburg ging es um die Website fashion.id. Mittlerweile muss die NutzerIn dort Social-Media-Dienste explizit aktivieren und stimmt damit zu, „dass Daten an die Betreiber der sozialen Netzwerke übertragen werden“. Insgesamt hatte die Verbraucherzentrale NRW im Frühjahr 2015 sechs Unternehmen wegen des „Like“-Buttons abgemahnt: HRS, Nivea (Beierdorf), Payback, Eventim, Fashion ID und KIK. Vier dieser Unternehmen hatten eine Unterlassungserklärung abgegeben. Ebenso uneinsichtig zeigte sich Payback, gegen das die VZ NRW beim LG München Klage eingereicht hat (Gericht gibt Verbraucherzentrale weitgehend recht, www.faz.net 09.03.2016; Verbraucherzentrale Nordrhein-Westfalen, PE: Facebook-Like-Button auf Firmen-Websites: Gericht rügt Datenschutzverstoß 09.03.2016).

AG Potsdam

Keine Kameradrohnen über Nachbars Garten

Gemäß einem Urteil des Amtsgerichts (AG) Potsdam vom 16.04.2015 gewährt die allgemeine Handlungsfreiheit keinen Anspruch darauf, eine Flugdrohne über das Grundstück des Nachbarn fliegen zu lassen (Az.: 37 C 454/13). In dem Fall ging es um einen Streit zwischen Nachbarn. Ein Mann hatte seine Drohne, die mit einer Kamera ausgestattet war, über das Haus und das Grundstück seiner Nachbarin fliegen lassen. Deren Grundstück ist durch hohe Hecken vor neugierigen Blicken geschützt. Als sie im Garten auf einer Sonnenliege las, startete der Nachbar seine Drohne. Die Nachbarin fühlte sich dadurch gestört und ließ den Piloten durch ihren Anwalt abmahnen und forderte die Abgabe einer Unterlassungserklärung. Als dieser dies verweigerte, zog sie vor Gericht.

Das AG gab der Frau Recht: Grundsätzlich sei der Luftraum für die vom Beklagten benutzte Drohne frei. Auch schütze die allgemeine Handlungsfreiheit die Pflege von eigenwilligen Hobbys. Doch hier gehe das im Grundgesetz geschützte Persönlichkeitsrecht vor. Zur Privatsphäre gehöre auch die Integrität eines nicht einsehbaren Gartens, der typischerweise ein Rückzugsort des Nutzenden ist. Beobachtungen anderer Personen seien als Ausspähung zu bewerten. Dies gelte umso mehr, wenn wie im vorliegenden Fall – einem offenkundig gestörten Nachbarschaftsverhältnis – das Fliegen der Drohne über dem Nachbargrundstück nicht mehr als zufällig erscheint. Vielmehr habe dies „bereits Züge von Mobbing“. Der Hinweis des Beklagten, er habe keine Aufnahmen vom Grundstück der Nachbarin gemacht und auch einen Abstand von 50 Metern zu dem betreffenden Grundstück eingehalten, konnte die Richter nicht überzeugen. Für sein Hobby gebe es genug andere Flächen. Es gehe nicht um ein Flugverbot oder um das „Untersagen einer kindlich-unschuldigen Freizeitbeschäftigung, wie beispielsweise einen Drachen steigen zu lassen oder ein Modellflugzeug zu

steuern“, sondern um eine Persönlichkeitsbeeinträchtigung.

Bei privater Nutzung darf der Flug nur innerhalb der Sichtweite der steuernden Person erfolgen. Auf freier Fläche entspricht dies einer maximalen Entfernung von 200 bis 300 Metern. Für Freizeitnutzungen sind keine Genehmigungen nötig, es sei denn, das Gerät wiegt mehr als 5 Kilogramm. Professionelle Fotografen, die aus kommerziellen Gründen Luftaufnahmen machen, bedürfen einer Behördenerlaubnis. (Drohnen dürfen nicht über Nachbargrundstück fliegen, www.berlin.de 01.02.2016; Nasemann, Ausgespäht, SZ 01.04.2016, 33).

SG Mainz

TK muss Versichertenpassfoto löschen

Das Sozialgericht (SG) Mainz entschied mit Urteil vom 01.12.2015, dass eine gesetzliche Krankenkasse das Foto eines Versicherten nach der Erfassung seiner Daten löschen muss (S 14 KR 477/15). Der Kläger hatte gegen die dauerhafte Speicherung seines Bildes geklagt und sich auf den Datenschutz und die informationelle Selbstbestimmung berufen. Eine Vorratsspeicherung für die Dauer der Mitgliedschaft sah er nicht für erforderlich an. Die Techniker Krankenkasse (TK) hatte sich geweigert, das Bild aus ihrer Datenbank zu nehmen – für den Fall, dass die von ihr herausgegebene elektronische Gesundheitskarte (eGK) verloren ginge oder zerstört würde. Eine Neubeschaffung des Fotos wäre mit einem unverhältnismäßigen Aufwand verbunden.

Der Vorsitzende Richter erklärte, er habe zwischen dem bürokratischen Aufwand für die Krankenkasse und dem Recht auf informationelle Selbstbestimmung des Klägers abwägen müssen. Die erstmalige Speicherung des Bildes für die eGK-Erstellung sei zulässig. Für die generelle Aufbewahrung des Fotos fehle jedoch die Rechtsgrundlage. Bei der Abwägung spielte auch die Frage, inwieweit die Fotos vor unbefugtem Zugriff Dritter geschützt sind, eine wichtige Rolle. Das SG kam zu dem Ergebnis, dass die Krankenkasse für eine neue Karte das Bild erneut vom Betroffenen einholen könne. Der Anwalt der beklagten TK erklärte: „Wir werden Ihr Foto umgehend löschen“. In der Regel löscht die TK die Daten ihrer Versicherten erst, wenn der Vertrag endet. Die eGK wurde in Deutschland seit 2011 stufenweise eingeführt; alle 5 Jahre muss sie erneuert werden.

Der Klägeranwalt kommentierte: „Das Gericht hat über einen Einzelfall entschieden“. Andere Betroffene könnten sich in Zukunft nicht auf diesen Prozess berufen. „Für die Versicherten bedeutet das Urteil womöglich, dass sie in Zukunft auf ihrem Antrag noch ein Häkchen mehr machen müssen“, für die Einwilligung nämlich, dass die Krankenkasse ihr Foto ohne zeitliche Einschränkung nutzen darf (Gesundheitskarte: Krankenkasse muss Foto löschen, www.haufe.de 02.12.2015; Hofer, Krankenkasse muss Foto für Gesundheitskarte löschen, CuA 2/2016, 19).

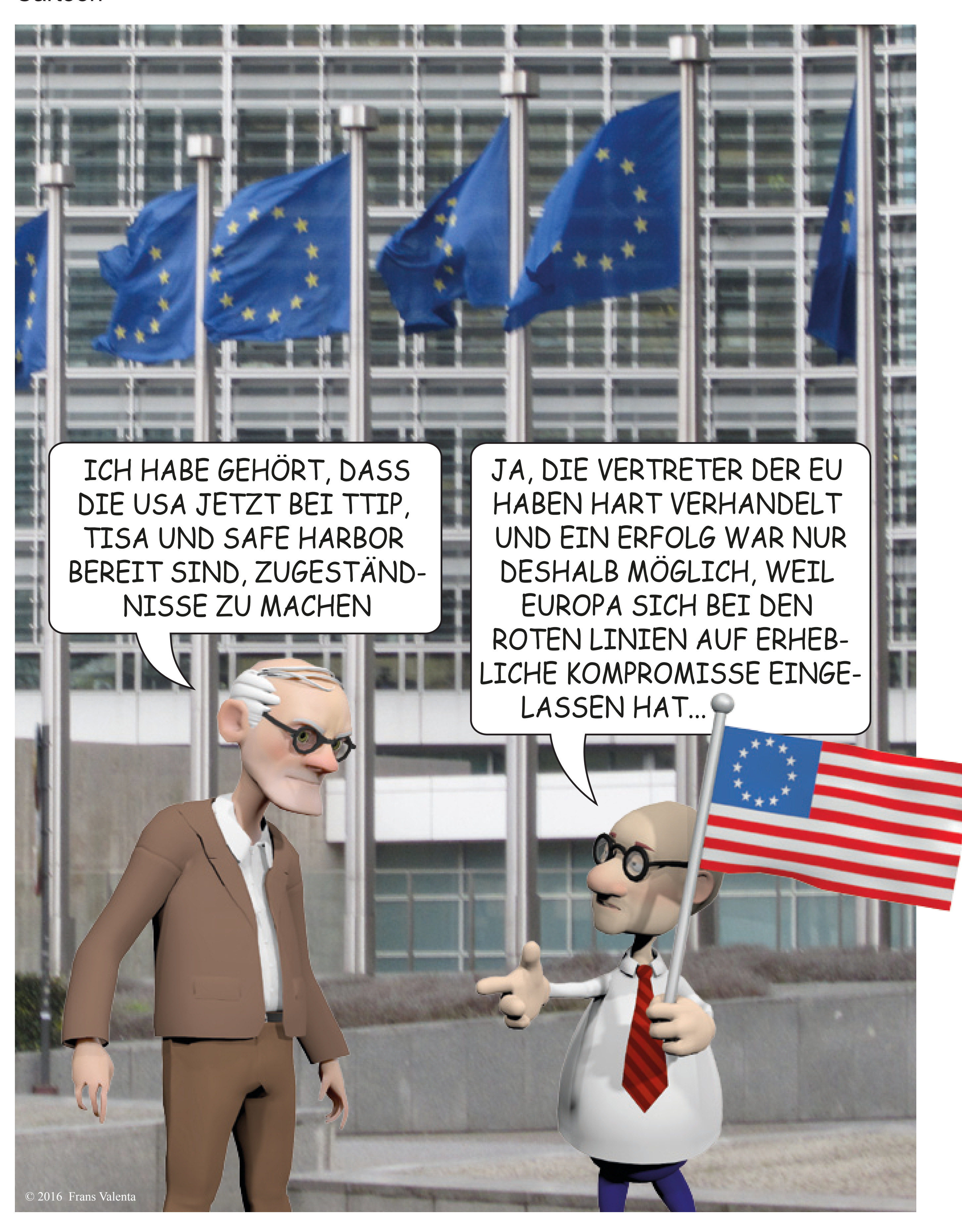
Buchbesprechungen



Datenschutz in der Kommunalverwaltung: Recht - Technik - Organisation
4., völlig neu bearbeitete Auflage
Erich Schmidt Verlag
ISBN 978 3 503 15664 1

(kn) Der neue Zilkens ist da – zu Recht hat sich das Werk aus dem Erich Schmidt Verlag als Standardlektüre für kommunale Datenschutzbeauftragte längst einen Namen gemacht. Auf 641 Seiten gelingt es hier dem langjährig erfahrenen Datenschutzpraktiker, in 15 Kapiteln nicht nur die datenschutzrechtlichen Grundbegriffe, Prinzipien und Systematiken abzubilden, sondern sich detailliert mit den besonderen Anforderungen in der kommunalen Praxis auseinanderzusetzen. Ein Überblick über den bereichsspezifischen Datenschutz fehlt dabei ebenso wenig, wie der kommunale Beschäftigtendatenschutz oder der Datenschutz im nichtöffentlichen Bereich des kommunalen Umfelds. Die bei dieser Themenfülle erforderliche Konzentration auf das Landesrecht NRW und ein systematisches Verständnis der Thematik kompensiert das Werk durch eine Fülle von hilfreichen Fußnotenverweisen auf weiterführende Informationsquellen. Gerade bei den technisch-organisatorischen Fragen entpuppt sich das scheinbar textlastige Werk als kompakte Arbeitshilfe für den Praktiker. Statt einer Fülle von Checklisten werden die rechtlichen Anforderungen mit praxisgerechten Beispielformulierungen begleitet. Der Autor vermeidet dabei auch nicht die Darstellung wichtiger Streitstände, was den Zilkens zu einem hilfreichen und kompakten Einsteigerwerk für die komplexen Themen des Datenschutzes auf Ebene der kommunalen Verwaltungen und für Praktiker aller Bundesländer empfehlenswert macht. Er sollte aber nicht nur im Regal jedes Datenschutzbeauftragten zu finden sein, sondern vor allem den Fachvorgesetzen den Einstieg in ihre Verantwortung erleichtern. Dieses Werk macht wie kaum ein anderes deutlich, dass der Datenschutz nicht als „Beauftragtenposition“ einem Datenschutzbeauftragten überlassen bleiben kann, sondern integraler Bestandteil einer modernen und rechtstaatlichen Verwaltungsarbeit ist.

Cartoon


ICH HABE GEHÖRT, DASS DIE USA JETZT BEI TTIP, TISA UND SAFE HARBOR BEREIT SIND, ZUGESTÄND-NISSE ZU MACHEN
JA, DIE VERTRETER DER EU HABEN HART VERHANDELT UND EIN ERFOLG WAR NUR DESHALB MÖGLICH, WEIL EUROPA SICH BEI DEN ROTEN LINIEN AUF ERHEB-LICHE KOMPROMISSE EINGE-LASSEN HAT...
© 2016 Frans Valenta